İSTİHBARAT TEORİSİ 2026

Bilişsel Harp, Yapay Zekâ, OSINT, Bayesçi Muhakeme ve Defansif Hibrit İstihbarat

“Yapay zekâ çağında istihbarat artık veri toplama değil, güvenilir karar mimarisi kurma disiplinidir.”

Bu çalışma; modern istihbarat düşüncesinin bilişsel harp, yapay zekâ, açık kaynak istihbaratı, Bayesçi muhakeme, siber-bilişsel operasyonlar ve hibrit tehditler karşısında geçirdiği dönüşümü incelemek amacıyla hazırlanmıştır.

Kitapta istihbarat yalnızca bilgi toplama faaliyeti olarak değil; belirsizlik altında karar üretme, tehditleri anlamlandırma, algı operasyonlarını çözümleme, veri yığınları içinden anlam çıkarma ve stratejik öngörü geliştirme disiplini olarak ele alınmaktadır.

Bu eser, akademik analiz ile pratik istihbarat düşüncesini bir araya getirerek, 2026 sonrası güvenlik ortamında istihbarat teorisinin nasıl yeniden okunması gerektiğine dair kapsamlı bir çerçeve sunar.

Çağdaş İNAL

Tüm hakları saklıdır.

Bu kitabın tamamı veya herhangi bir bölümü, yazarın yazılı izni olmadan çoğaltılamaz, dağıtılamaz, dijital ortama aktarılamaz veya ticari amaçla kullanılamaz.

EVENTICA Yayınları

Birinci Dijital Baskı

2026

Okuyucu İçin Hızlı Başlangıç

Bu bölüm, kitabın neyi çözdüğünü, kime hitap ettiğini ve okuyucuya ne kazandıracağını hızlıca görmek isteyenler için hazırlanmıştır.

Bu kitap hangi problemi çözüyor?

Bu kitap, yapay zekâ çağında istihbaratın yalnızca veri toplama faaliyeti olarak okunmasının artık yetersiz kaldığını gösterir. Asıl problemi; veri bolluğu, bilgi kirliliği, bilişsel harp, algoritmik manipülasyon, açık kaynakların yükselişi ve belirsizlik altında karar üretme ihtiyacı üzerinden ele alır. Okuyucuya, modern istihbaratı güvenilir karar mimarisi kurma disiplini olarak yeniden düşünme imkânı sunar.

Kim okumalı?

Güvenlik çalışmaları, uluslararası ilişkiler, kamu politikası, savunma sanayii, siber güvenlik, OSINT, yapay zekâ yönetişimi, stratejik iletişim ve risk analizi alanlarıyla ilgilenen öğrenciler, araştırmacılar, analistler ve karar vericiler için hazırlanmıştır. Teknik okur da akademik okur da kitabı farklı seviyelerde kullanabilir.

Okuyucu kitabı bitirince ne kazanacak?

Okuyucu; bilişsel harp, yapay zekâ destekli analiz, OSINT, Bayesçi muhakeme, siber-bilişsel tehditler ve defansif hibrit istihbarat kavramlarını tek bir bütün içinde okuyabilecek. Ayrıca hangi bilginin güvenilir, hangi verinin yanıltıcı, hangi analitik sonucun hukuken ve etik olarak savunulabilir olduğunu değerlendirmek için daha sağlam bir düşünme çerçevesi kazanacaktır.

Bu kitap piyasadaki diğer kitaplardan neden farklı?

Bu çalışma, klasik istihbarat anlatısını yalnızca tarihsel ve kurumsal düzeyde bırakmaz; yapay zekâ, OSINT, ticari veri, platform algoritmaları, bilişsel harp, Bayesçi güncelleme ve 2030'a uzanan defansif hibrit istihbarat mimarisini aynı teorik hatta birleştirir. Bu yönüyle yalnızca "istihbarat nedir?" sorusuna değil, "istihbarat yapay zekâ çağında nasıl yeniden kurulmalıdır?" sorusuna da cevap arar.

Kitabın Cevapladığı Stratejik Sorular

Aşağıdaki sorular, kitabın ana tartışma hattını sade biçimde özetler. Her bölüm bu soruların farklı bir katmanını açar ve okuyucuyu 2026 sonrası güvenlik ortamını daha geniş bir gözle okumaya çağırır.

“Yapay zekâ çağında istihbarat nasıl değişiyor?”

İstihbarat, yapay zekâ çağında hızlanan veri işleme kapasitesiyle birlikte daha fazla otomasyona, daha fazla doğrulama ihtiyacına ve daha güçlü insan denetimine ihtiyaç duyar. Yapay zekâ analiz süreçlerini hızlandırabilir; fakat kaynağı belirsiz veri, otomasyon yanlılığı, model hataları ve sentetik içerik riski nedeniyle istihbaratın merkezinde hâlâ insan muhakemesi, kanıt disiplini ve etik denetim bulunmalıdır.

“Bilişsel harp artık sadece devletlerin değil toplumların da meselesi mi?”

Evet. Bilişsel harp artık yalnızca devlet kurumlarını veya askerî karar vericileri hedef alan dar bir alan değildir. Toplumların dikkat ekonomisi, güven ilişkileri, kimlik algısı, haber tüketimi ve platform davranışları da bu alanın parçasıdır. Bu nedenle bilişsel güvenlik, sadece savunma kurumlarının değil; medya, eğitim, teknoloji şirketleri, kamu kurumları ve bireylerin de ortak sorumluluğudur.

“OSINT ve ticari veri güvenlik alanını nasıl dönüştürüyor?”

OSINT ve ticari veri, güvenlik alanında sensör sayısını, kaynak çeşitliliğini ve analiz hızını artırır. Uydu görüntüleri, sosyal medya verileri, açık devlet kayıtları, ticari veri setleri ve dijital izler; krizleri, çatışmaları, afetleri ve etki operasyonlarını daha görünür hâle getirir. Ancak bu dönüşüm aynı zamanda mahremiyet, veri kalitesi, kaynak doğrulama, ticari bağımlılık ve hukuki denetim sorunlarını da büyütür.

“Türkiye 2030’a giderken nasıl bir defansif hibrit istihbarat mimarisi kurmalı?”

Türkiye için 2030’a giden hatta en sağlam yaklaşım; siber güvenlik, OSINT, yapay zekâ, hukuk, etik denetim, kriz yönetimi, stratejik iletişim ve kurumsal dayanıklılığı aynı mimaride birleştiren defansif hibrit istihbarat modelidir. Bu model, tek merkezli kapalı bir yapıdan çok; ortak standartlara, denetlenebilir veri kullanımına, çok dilli analiz kapasitesine, yerli yapay zekâ test altyapısına ve kurumlar arası güvenilir iş birliğine dayanmalıdır.

Bölüm Okuma Şablonu

Daha verimli olması için her bölüm şu yapıya çekilmeli:

• Bölümün kısa problemi: Bölüm başlamadan önce okuyucuya hangi sorunun çözüleceği net biçimde gösterilmelidir.

• Ana kavramlar: Bölümde kullanılan temel terimler kısa, tutarlı ve tekrar kontrol edilebilir şekilde verilmelidir.

• Gerçek dünya bağlantısı: Teorik anlatım; güncel vaka, kurum, teknoloji veya güvenlik olayıyla desteklenmelidir.

• Model / tablo / şekil: Her bölümde karmaşık yapıyı sadeleştiren en az bir analitik model, tablo veya şekil bulunmalıdır.

• Riskler: Teknik, hukuki, etik, kurumsal ve stratejik riskler ayrı ayrı görünür hale getirilmelidir.

• Türkiye açısından anlamı: Bölümdeki kavramların Türkiye'nin güvenlik, teknoloji, hukuk ve kurumsal kapasite alanlarına etkisi ayrıca değerlendirilmelidir.

• 5 maddelik bölüm sonucu: Okuyucu bölüm sonunda ana çıkarımları hızlıca görebilmelidir.

• Okuma soruları: Bölüm, tartışma veya eğitim ortamında kullanılabilecek kısa sorularla kapanmalıdır.

• Kaynakça: Bölümde kullanılan ana kaynaklar düzenli, doğrulanabilir ve tek biçimli kaynakça standardına uygun verilmelidir.

Bu şablon, kitabı yalnızca okunacak bir metin olmaktan çıkarıp eğitim, analiz, tartışma ve yeniden kullanım açısından daha verimli bir referans kaynağına dönüştürür.

Kitabın Adı: İstihbarat Teorisi 2026
Alt Başlık: Bilişsel Harp, Yapay Zekâ, OSINT, Bayesçi Muhakeme ve Defansif Hibrit İstihbarat
Yazar: Çağdaş İnal
Yayıncı: EVENTICA Yayınları
Yayın Türü: E-Kitap
Dil: Türkçe
Birinci Dijital Baskı: 2026
Yayın Yeri: Türkiye
ISBN / e-ISBN: 979-8-2409-3055-3
Yazar E-Posta: cagdasinal80@gmail.com
Kitap E-Posta: **yayin@eventicayayinlari.com.tr**
Kitap Web Sitesi: http://www.istihbaratteorisi.com.tr/
Yayıncı E-Posta: iletisim@istihbaratteorisi.com.tr
Yayıncı Web Sitesi: http://www.eventicayayinlari.com.tr/

© 2026 Çağdaş İNAL. Tüm hakları saklıdır.

Bu kitabın tamamı veya herhangi bir bölümü, yazarın ve yayıncının yazılı izni olmadan çoğaltılamaz, dağıtılamaz, ticari amaçla kullanılamaz, dijital ortamlarda yeniden yayınlanamaz veya herhangi bir veri tabanı, yapay zekâ eğitim seti ya da içerik üretim sistemi içinde izinsiz şekilde işlenemez.

Bu eser, EVENTICA Yayınları tarafından dijital yayıncılık formatına uygun şekilde yayınlanmak üzere hazırlanmıştır.

İletişim: cagdasinal80@gmail.com
Web: http://www.istihbaratteorisi.com.tr/

EVENTICA Yayınları Hakkında

EVENTICA Yayınları, Çağdaş İNAL tarafından kurulan bağımsız bir dijital yayın ve e-kitap markasıdır. Akademik, kültürel, stratejik, teknolojik, araştırma ve düşünce odaklı eserleri okuyucuyla buluşturmayı amaçlar.

Yayın anlayışı; özgün içerik, editoryal bütünlük, telif haklarına saygı, güvenilir kaynak kullanımı ve dijital yayıncılık standartlarına uygunluk üzerine kuruludur.

EVENTICA Yayınları ilk aşamada e-kitap formatında yayın yapmayı, eserlerini dijital platformlar üzerinden okuyucuya ulaştırmayı hedeflemektedir. İlerleyen süreçte ise basılı yayıncılık alanında da faaliyet gösterilmesi planlanmaktadır.

Yayıncı iletişim adresleri: cagdasinal80@gmail.com, yayin@eventicayayinlari.com.tr, iletisim@istihbaratteorisi.com.tr

Resmî web sitesi: http://www.eventicayayinlari.com.tr/

Yasal ve Etik Kullanım Uyarısı

Bu kitap, istihbarat teorisi, açık kaynak analizi, yapay zekâ destekli karar süreçleri, bilişsel harp, siber-bilişsel güvenlik ve hibrit tehditler üzerine akademik ve analitik bir çalışma olarak hazırlanmıştır.

Kitapta yer alan bilgiler eğitim, araştırma, stratejik analiz, kuramsal değerlendirme ve farkındalık amacı taşır. Buradaki kavramlar, yöntemler ve analiz çerçeveleri herhangi bir yasa dışı faaliyet, yetkisiz erişim, kişisel veri ihlali, saldırı, gözetim, manipülasyon veya zarar verici operasyon amacıyla kullanılmamalıdır.

Okuyucu, kitapta yer alan bilgileri yürürlükteki hukuk kuralları, etik ilkeler, kişisel haklara saygı, mahremiyet ve kamu güvenliği çerçevesinde değerlendirmekle sorumludur. Yazar ve yayıncı, bu eserde yer alan bilgilerin hukuka aykırı, izinsiz, saldırgan veya zarar verici amaçlarla kullanılmasından sorumlu değildir.

Önsöz

İstihbarat artık yalnızca gizli bilgiye ulaşma meselesi değildir. Modern dünyada asıl mesele; veri bolluğu içinde anlam üretebilmek, belirsizlik altında karar verebilmek, yapay zekâ destekli sistemlerin ürettiği sonuçları

sorgulayabilmek ve insan zihnini hedef alan yeni tehdit biçimlerini anlayabilmektir.

Bu kitap, istihbaratı klasik tanımının ötesinde ele alır. Açık kaynak istihbaratı, bilişsel harp, yapay zekâ, Bayesçi muhakeme, siber-bilişsel operasyonlar, hibrit tehditler ve defansif istihbarat yaklaşımı aynı bütün içinde değerlendirilmiştir.

Amaç, okuyucuya sadece kavramları anlatmak değildir. Amaç; modern güvenlik ortamında bilginin nasıl üretildiğini, nasıl manipüle edildiğini, nasıl analiz edildiğini ve karar süreçlerine nasıl dönüştüğünü daha geniş bir çerçeveden göstermektir.

İstihbarat Teorisi 2026, bu yönüyle hem akademik hem de pratik düşünceye yakın duran bir çalışmadır. Kitap; öğrenciler, araştırmacılar, analistler, güvenlik çalışmalarıyla ilgilenen okuyucular ve teknolojinin stratejik sonuçlarını anlamak isteyen herkes için hazırlanmıştır.

Çağdaş İNAL
2026

Kısaltmalar

AGI	Genel Yapay Zekâ
AI	Artificial Intelligence / Yapay Zekâ
CTI	Siber Tehdit İstihbaratı
DHI	Defansif Hibrit İstihbarat
DISARM	Dezenformasyon ve etki operasyonlarını analiz etmeye yönelik çerçeve
DSS	Karar Destek Sistemi
FIMI	Dış Bilgi Manipülasyonu ve Müdahalesi
GEOINT	Coğrafi İstihbarat
HUMINT	İnsan Kaynaklı İstihbarat
IMINT	Görüntü İstihbaratı
LLM	Büyük Dil Modeli
OODA	Gözlem, Yönelim, Karar, Eylem Döngüsü
OSINT	Açık Kaynak İstihbaratı
PAI	Kamuya Açık Bilgi

SOCMINT	Sosyal Medya İstihbaratı
YZ	Yapay Zekâ

İçindekiler

Başlık Sayfa

Künye / Telif Bilgileri ..... Sayfa 2
EVENTICA Yayınları Hakkında ..... .Sayfa 3
Yasal ve Etik Kullanım Uyarısı ..... Sayfa 3
Önsöz ..... Sayfa 3
Kısaltmalar ..... Sayfa 4
İçindekiler ..... Sayfa 5
Şekiller Listesi ..... Sayfa 6
Tablolar Listesi ..... Sayfa 6
Formüller Listesi .....Sayfa 6
Editoryal Not ve Üretim Mantığı .....Sayfa 7
Yöntem, Standartlaştırma ve Okuma Kılavuzu ..... Sayfa 9
Terminoloji Standardizasyonu ..... Sayfa 9
Yönetici Özeti .....Sayfa 10

Bölüm 1. İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp .....Sayfa 26
Bölüm 2. Sistemik İnvariantlar ve Sosyal Sistemlerin Hedef Alınması ....Sayfa 58
Bölüm 3. Yapay Zekâ Destekli Tahmin Sistemleri ve Makine Hızında Karar Alma..... Sayfa 76
Bölüm 4. OSINT, Veri Mühendisliği Boru Hatları ve LLM Ajanları ..... Sayfa 98
Bölüm 5. Davranışsal Modelleme ve Ajan Tabanlı Simülasyonlar ..... Sayfa 120
Bölüm 6. Siber-Bilişsel Kesişimde FIMI ve DISARM Çerçevesi ..... Sayfa 132
Bölüm 7. Otonom Hedefleme ve Karar Destek Sistemleri ..... Sayfa 146
Bölüm 8. Bayesçi İstihbarat: Kanıt, Olasılık ve Hipotez Güncelleme .....

Sayfa 159
Bölüm 9. Makine Öğrenmesinin İstihbari Epistemolojisi .....
Sayfa 164
Bölüm 10. Teknolojik Trendler, AGI Projeksiyonları ve Caydırıcılık Boşluğu.....
Sayfa 178
Bölüm 11. Sosyal Sistemlere Yönelik İstihbarat ve Kurumsal Dayanıklılık .....
Sayfa 194
Bölüm 12. Hibrit İstihbarat ve Nöro-Bilişsel Savunma .....
Sayfa 205
Bölüm 13. Stratejik Sonuçlar, DHI Yol Haritası ve 2030 Kapanışı .....
Sayfa 221

Ek C. Editoryal Üretim ve Kaynak Kullanım Notu .....
Sayfa 223
Kaynakça ve Seçilmiş Okuma Listesi .....
Sayfa 230
Ekler .....
Sayfa 237
Ek A. Kavram Sözlüğü .....
.....Sayfa 237
Kaynak Dosya Havuzu ve İnternet Destekli Kaynaklar .....
Sayfa 238
Kapanış Notu .....
Sayfa 239

Şekiller Listesi

Şekil 1. Klasik çevrimden ağ tabanlı istihbarat işletim sistemine geçiş
..... .Sayfa 8
Şekil 2. İstihbarat döngüsünün işletim sistemi mantığına
evrilmesi .....Sayfa 26
Şekil 3. Sosyal sistemlerin korunması gereken invariant
yapıları .....Sayfa 58
Şekil 4. Makine hızında karar mimarisinde hız ve doğruluk
gerilimi ..... Sayfa 76
Şekil 5. OSINT verisinin karar ürününe dönüşme
hattı ..... Sayfa 98
Şekil 6. FIMI/DISARM analizinde saldırı ve savunma döngüsü .....
Sayfa 133
Şekil 7. DSS içinde insan denetimi, hız ve hukuk
filtresi ..... Sayfa 146
Şekil 8. Bayesçi hipotez güncelleme
döngüsü ..... Sayfa 159
Şekil 9. Makine öğrenmesi kaynaklı epistemolojik risk
hattı ..... Sayfa 164
Şekil 10. Sosyal sistem dayanıklılığının analiz omurgası .....
.Sayfa 194
Şekil 11. Defansif Hibrit İstihbarat
mimarisi ..... Sayfa 206

Şekil 12. Kitabın stratejik kapanışında DHI merkezli kurumsal dönüşüm ..... Sayfa 221

Tablolar Listesi

Tablo 1. Kitap omurgası ve kaynak eşleştirmesi ....Sayfa 8
Tablo 2. Terminoloji standardizasyonu ..... Sayfa 9
Tablo 3. Bölüm 1 hızlı okuma haritası ..... Sayfa 26
Tablo 4. Bilişsel harp ile klasik bilgi harekâtı ayrımı ..... Sayfa 26
Tablo 5. Sistemik invariant sınıflandırması ..... Sayfa 58
Tablo 6. YZ tahmin sistemlerinde ana risk alanları ..... Sayfa 76
Tablo 7. OSINT boru hattı kalite kontrolleri ..... Sayfa 98
Tablo 8. Ajan tabanlı modelleme kullanım haritası ..... Sayfa 120
Tablo 9. FIMI analiz katmanları ..... Sayfa 133
Tablo 10. DSS tasarımında kontrol matrisi ..... Sayfa 146
Tablo 11. Bayes formülünün istihbarattaki karşılığı ..... Sayfa 159
Tablo 12. Epistemolojik patolojiler ..... Sayfa 164
Tablo 13. Caydırıcılık boşluğunu büyüten faktörler ..... Sayfa 178
Tablo 14. Kurumsal dayanıklılık göstergeleri ..... Sayfa 194
Tablo 15. DHI alanları ve görevleri ....Sayfa 206
Tablo 16. 2030 yol haritası ..... Sayfa 221
Tablo 17. Genişletilmiş kavram sözlüğü ..... Sayfa 237
Tablo 18. Kullanılan dosyalar ..... Sayfa 238

Formüller Listesi

Formül 1. POMDP gösterimi: POMDP = (S, A, T, R, Ω, O, γ) ..... Sayfa 80
Formül 2. Shannon Entropisi: $H(X) = -\Sigma_i\, p(x_i)\, \log_2 p(x_i)$ ....Sayfa 101
Formül 3. XGBoost objektif fonksiyonu: $Obj = \Sigma_i\, l(y_i, \hat{y}_i) + \Sigma_k\, \Omega(f_k)$ ..... Sayfa 102
Formül 4. XGBoost düzenlileştirme terimi: $\Omega(f) = \gamma T + 1/2\, \lambda \|w\|^2$ .....

Sayfa 102
Formül 5. Etkileşim Verimliliği: EV = (Σᵢ wᵢ × rᵢ) / C ..... Sayfa 135
Formül 6. Bayes formülü: P(H|E) = [P(E|H) × P(H)] / P(E) ..... Sayfa 160
Formül 7. Rashomon kümesi: Rε = { f ∈ F | L(f) ≤ L(f*) + ε } ..... Sayfa 166

Editoryal Not ve Üretim Mantığı

Bu kitap, modern istihbaratı tek bir dar faaliyet alanı olarak değil; veri, insan muhakemesi, yapay zekâ, sosyal sistemler, bilişsel güvenlik, hukuki denetim ve stratejik karar alma arasında kurulan canlı bir mimari olarak ele alır. Klasik anlamda istihbarat, gizli bilgiyi toplama ve bu bilgiyi karar vericiye taşıma işiydi. 2026 dünyasında bu tanım artık eksik kalıyor. Çünkü karar üstünlüğü sadece daha fazla veri toplamakla değil; verinin nereden geldiğini bilmekle, hangi bağlamda anlam kazandığını çözmekle, hangi hipotezi ne kadar güçlendirdiğini hesaplamakla ve bu süreci hukuken, etik olarak ve kurumsal olarak savunulabilir hale getirmekle kuruluyor.

Bu yüzden kitapta ana kavramlar tek bir çizgiye çekildi: “cognitive warfare” karşılığı olarak “bilişsel harp”, “hybrid intelligence” karşılığı olarak “hibrit istihbarat”, “machine learning” karşılığı olarak “makine öğrenmesi”, “artificial intelligence” karşılığı olarak ise ilk kullanımda “yapay zekâ / YZ” tercih edildi. İngilizce kısaltmalar ilk geçtiği yerde açıklandı; sonraki bölümlerde Türkçe kavram ana gövdeye yerleştirildi. Böylece metin hem akademik çizgisini korudu hem de okunur kaldı.

Bu çalışma kısa bir rapor değildir. Bölümler arasında tekrar eden kavramsal girişler temizlendi; fakat özgün analizler, tablolar, vaka bağlantıları, sistem mimarileri, risk değerlendirmeleri ve stratejik sonuçlar korunarak genişletildi. Amaç sayfa azaltmak değil; dağınık bölüm taslaklarını, araştırma notlarını ve kaynak dosyalarını tek bir final kitap omurgasına bağlamaktır.

Klasik çevrimden istihbarat işletim sistemine geçiş

Şekil 1. Klasik çevrimden ağ tabanlı istihbarat işletim sistemine geçiş

Tablo 1. Kitap omurgası ve kaynak eşleştirmesi

Bölüm	Ana konu	Birleştirilen kaynak havuzu
1	Ontolojik dönüşüm ve bilişsel harp	İstihbaratın Ontolojik Dönüşümü; Bilişsel Harp raporları
2	Sistemik invariantlar	Sosyal Sistemlere Yönelik İstihbarat Analizi
3	YZ destekli tahmin sistemleri	Yapay Zekâ Tahmin Sistemleri Stratejik Analizi
4	OSINT ve veri mühendisliği	OSINT, LLM ve Stratejik İstihbarat Analizi
5	Davranışsal modelleme	Davranışsal Modelleme ve YZ Simülasyonları
6	FIMI ve DISARM	Siber-Bilişsel FIMI / DISARM Çerçevesi
7	DSS ve otonom hedefleme	Otonom Hedefleme ve DSS Araştırma Raporu
8	Bayesçi istihbarat	Yeni eklenen analitik

Bölüm	Ana konu	Birleştirilen kaynak havuzu
		bölüm
9	Makine öğrenmesi epistemolojisi	Makine Öğrenmesi İstihbarat Epistemolojisi
10	AGI ve caydırıcılık boşluğu	AGI, Hibrit Tehditler ve Caydırıcılık Analizi
11-13	DHI ve stratejik kapanış	Hibrit İstihbarat ve Nöro-Bilişsel Savunma Analizi + sentez

Yöntem, Standartlaştırma ve Okuma Kılavuzu

Kitabın üretim mantığı üç aşamaya dayanır. İlk aşama kavramsal standardizasyondur. Aynı kavram farklı dosyalarda farklı adlarla geçtiğinde, terim tekleştirildi ve ilk kullanımda parantez içinde alternatifleri gösterildi. İkinci aşama mimari bütünleştirmedir. Ontoloji, sosyal sistemler, OSINT, yapay zekâ, DSS, FIMI, AGI ve nöro-bilişsel savunma bölümleri aynı stratejik hat üzerinde yeniden sıralandı. Üçüncü aşama akademik kitaplaştırmadır. Her bölüm kendi kavramsal çerçevesi, sistem modeli, risk analizi, tablo/diyagram desteği ve sonuç çıkarımıyla düzenlendi.

Bu metindeki yaklaşım şudur: istihbarat sadece “ne oldu?” sorusuna cevap vermez. İyi istihbarat “bunu nereden biliyoruz?”, “ne kadar emin olabiliriz?”, “hangi veri bizi yanıltıyor olabilir?”, “hangi hipotez daha güçlendi?”, “hangi karar eşiğinde hareket etmeliyiz?” sorularını birlikte taşır. Bayesçi muhakeme bölümü bu yüzden ayrı bir bölüm olarak eklendi. Çünkü çağdaş istihbaratta belirsizlik yok sayılmaz; ölçülür, güncellenir ve karar sürecine disiplinli biçimde aktarılır.

Tablo 2. Terminoloji standardizasyonu

Standart terim	Kullanım ilkesi
Bilişsel Harp	Algı, dikkat, güven, muhakeme, kimlik ve karar süreçlerini hedef alan çatışma biçimi.
FIMI	Dış Bilgi Manipülasyonu ve Müdahalesi; dış aktör kaynaklı koordineli bilgi manipülasyonu.
DHI	Defansif Hibrit İstihbarat; siber, bilişsel, hukuki, algoritmik ve tedarik zinciri risklerini birlikte ele alan savunma yaklaşımı.
OSINT	Açık kaynaklardan üretilen istihbarat; kamusal ve bazı ticari erişilebilir veri katmanlarını kapsar.
DSS	Karar Destek Sistemi; insan karar vericiye seçenek, risk ve öncelik üreten analitik mimari.
OODA	Gözlem, Yönelim, Karar, Eylem döngüsü; modern yapıda doğrusal değil ağ tabanlı çalışır.
Bayesçi Güncelleme	Yeni kanıtla hipotez olasılığının sistematik biçimde güncellenmesi.
Rashomon Etkisi	Aynı veri setini açıklayan birden fazla tutarlı modelin bulunması durumu.
Ajan Yapay Zekâ	Hedefleri alt görevlere bölebilen, araç kullanabilen ve sınırlı otonomiyle ilerleyebilen YZ yapısı.
Sistemik İnvariant	Bir sosyal sistemin şoklara rağmen kimliğini ve koordinasyon kapasitesini koruyan değişmez yapı taşı.

İstihbarat Teorisi 2026 Yönetici Özeti Bu rapor, mevcutlar kullanıcı tarafından belirlenmiş özgün Bölüm başlıkları paylaşılmadığı için,

“**İstihbarat Teorisi 2026**” EPIC’ini alan yazın ve kurumsal doktrinler temelinde yeniden yapılandırılmış bölüm bir çerçeve olarak ele alır. Bu yeniden kurgu, klasik istihbarat kuramını; açık kaynak, ticari veri, geo uzamsal istihbarat, siber tehdit istihbaratı, yapay zekâ, gözetim teknolojileri, propaganda algoritmaları ve hukuk-etik yönetişimi ile birleştirmeyi amaçlar. Güncel literatürün ana bulgusu nettir: istihbarat artık yalnızca “gizli olanı bulma” işi değildir; kamusal ve ticari veriden karar üstünlüğü üretme, çok disiplinli füzyon yapma ve bu füzyonu hukuken savunulabilir hale getirme işidir. ODNI’nin OSINT stratejisi açık kaynağı “yaşamsal” bir kabiliyet olarak tanımlarken, Türkçe tarafta Milli İstihbarat Akademisi de OSINT, siber güvenlik ve istihbarat çalışmaları alanında kurumsal profesyonelleşme ihtiyacını sistematik biçimde tartışmaktadır. [1]

Stratejik tabloyu değiştiren temel kırılma, açık ve ticari verinin ölçek, hız ve çeşitlilik bakımından klasik istihbarat çevrimini yeniden kurmasıdır. 2024 tarihli IC OSINT Strategy, OSINT’i yalnızca kamusal değil ticari olarak erişilebilen bilgiye dayanan ayrı bir üretim hattı olarak kurumsallaştırırken, ODNI’nin 2024 Ticari Olarak Erişilebilir Bilgi çerçevesi bu alanın mahremiyet ve sivil özgürlük riskleri için ortak bir asgari yönetişim tabanı getirmiştir. Aynı dönemde yeni standartlar, OSINT/PAI/CAI ürünlerinde kaynaklandırma ve izlenebilirlik gerekliliklerini sıkılaştırmıştır. [2] İkinci büyük kırılma, GEOINT ve siber istihbaratın büyük ölçüde ticarileşmesi ve modülerleşmesidir. NGA, GEOINT’i ulusal güvenlik için görüntü ve coğrafi verinin işletilmesi ve analizi olarak tanımlarken; Copernicus, Landsat, Planet ve Maxar gibi ekosistemler savaş, afet ve kritik altyapı gözetiminde “açık/ticari sensör katmanı”nı kalıcı hale getirmiştir. Rusya-Ukrayna savaşı, ticari uydu görüntülerinin hem savaşın belgelendirilmesinde hem de kamuoyu algısının şekillenmesinde belirleyici olduğu ilk büyük örnek olarak öne çıkmıştır; 2025’te GEGD/Maxar erişiminin askıya alınması ise ticari bağımlılığın jeopolitik bir risk olduğu gerçeğini ortaya koymuştur.

Siber tarafta MITRE ATT&CK, STIX/TAXII ve MISP tabanlı CTI paylaşımı standardize olurken Volt Typhoon ve Salt Typhoon olayları, kritik altyapı ve telekom omurgalarına karşı uzun vadeli ön-konumlanmanın başlıca tehdit modeli olduğunu göstermiştir. [3] Üçüncü kırılma, yapay zekânın iki yönlü etkisidir: istihbarat üretimini hızlandırırken denetlenebilirlik, güvenilirlik ve

hak temelli yönetişim sorunlarını büyütmektedir. NIST AI RMF ve 2024 üretken yapay zekâ profili, kurumlara güvenilir AI için gönüllü fakat ayrıntılı bir risk yönetim modeli sunar; AB AI Act ise 1 Ağustos 2024'te yürürlüğe girmiş ve 2 Ağustos 2026'ya giden kademeli uygulama takvimiyle yüksek riskli kullanımları regüle etmeye başlamıştır. Aynı anda mercenary spyware ekosistemi derinleşmiş; Apple'ın tehdit bildirimleri, Paragon Graphite vakaları, Intellexa/Predator yaptırımları ve Citizen Lab'in 2026 tarihli ad-temelli konum gözetimi raporu, istihbarat ile gözetim-capitalism arakesitinin ne kadar hızlı genişlediğini göstermiştir. Stanford AI Index 2026'nın işaret ettiği gibi yetenek artışı ile yönetişim hazırlığı arasındaki makas açılmaktadır.

[4] Türkiye bakımından en önemli sonuç şudur: strateji belgeleri ve kurumsal farkındalık artmış durumdadır; ancak kamuya açık doktrin, standartlaştırılmış kaynaklandırma, Türkçe ve bölgesel diller için veri/AI altyapısı, ticari veri tedarik rejimi, üniversite-kurum-sanayi arasında müşterek eğitim boru hattı ve demokratik denetim mimarisi hâlâ parçalı görünmektedir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028, UYZS 2021-2025, USOM altyapısı, KVKK rehberleri ve MİA yayınları değerli bir temel sağlamaktadır; fakat bunların müşterek bir "istihbarat mimarisi"ne dönüştürülmesi bu EPIC'in asıl stratejik amacıdır. [5] Yöntem ve Varsayımlar Bu çalışma, kullanıcı tarafından belirlenmiş orijinal dosya listesinin mevcut yapısında yer almaması nedeniyle, alanı kapsayıcı olacak biçimde önerilmiş bir bölüm mimarisi kurar. Hedef kitle, süre ve değerlendirme biçimi de kullanıcı mesajında belirtilmemiştir. Bu nedenle rapor, üç makul kullanım senaryosu varsayar: karar alıcılara yönelik kısa sertifika, analistlere yönelik uygulamalı meslek içi program ve lisansüstü/seminer formatı. Her bölümiçin önerilen modül, bu üç senaryodan herhangi birine ölçeklenebilir şekilde tasarlanmıştır.

Kaynak önceliği şu sırayla verilmiştir: resmi/kurumsal doktrin ve stratejiler; birincil teknik/standart belgeler; hakemli akademik yayınlar; büyük teknoloji veya güvenlik sağlayıcılarının şeffaflık ve teknik dokümanları; Türkçe resmi raporlar ve düşünce kuruluşu analizleri. Bu nedenle ODNI, NIST, CISA, NGA, Avrupa Komisyonu, Apple, U.S. Treasury, FBI, UK doctrine kaynakları; Türkiye tarafında Ulaştırma ve Altyapı Bakanlığı,

USOM, KVKK, BTK, UYZS belgeleri ve Milli İstihbarat Akademisi yayınları raporun ana omurgasını oluşturur. 2020-2026 dönemi özellikle vurgulanmıştır; çünkü bu dönem açık kaynak profesyonelleşmesi, ticari veri yönetişimi, AI düzenlemesi, mercenary spyware yayılımı ve platform algoritmalarının siyasal etkileri bakımından yapısal bir geçiş dönemi olmuştur. [6] Varsayımsal modül ölçeği için en dengeli seçenek, her bölümiçin 6 saat ders + 4 saat laboratuvar + 2 saat değerlendirme toplamı 12 saatlik bir yapı görünmektedir. Daha kısa programlarda her bölüm3-6 saatlik yoğunlaştırılmış oturuma; lisansüstü programlarda ise bir haftalık veya iki haftalık bloklara dönüştürülebilir.

Analist eğitimi literatürü, yalnızca teorik içerikten çok vaka-temelli ve ürün-temelli eğitimlerin uyarı zekâsı, analitik muhakeme ve kurumsal profesyonelleşme bakımından daha etkili olduğunu göstermektedir. [7] bölümHaritası ve Bağımlılıklar Aşağıdaki mimari, on sprinti birbirinden kopuk modüller olarak değil, kuramdan toplama disiplinlerine, oradan füzyon, yönetişim ve Türkiye'ye özgü kurumsal mimariye giden tek bir bütünleşik hat olarak ele alır. Özellikle güncel doktrinler ve OSINT/CAI yönetişimi, istihbaratın artık "gizli veri ağırlıklı bir uzmanlık" değil, çok kaynaklı kanıt üretimi ve izlenebilir karar desteği işi haline geldiğini göstermektedir. [8] Aşağıdaki ilişki şeması, on bölümarasındaki ardışık bağımlılıkları gösterir. Özellikle bölüm5-9 aralığı teknik görünse de, bunların güvenilir biçimde işletilebilmesi için bölüm1-4'teki analitik ve örgütsel temel şarttır; bölüm10 ise bütün hattın hukuki-etik "fren ve direksiyon" sistemidir. Bu okuma, güncel doktrin ve yönetişim belgeleriyle uyumludur.

[9] 2020-2026 döneminin kritik eşikleri, bu EPIC'in neden "2026" başlığını hak ettiğini de gösterir: 2020'de DoD veri ve PAI yaklaşımlarını güncelledi; 2021'de STIX/TAXII 2.1 yayımlandı ve Türkiye UYZS 2021-2025'i devreye aldı; 2022'de Rusya-Ukrayna savaşı ticari görüntü istihbaratını merkezî hale getirdi; 2023-2025 arasında Volt/Salt Typhoon, mercenary spyware ve platform etkisi tartışmaları yoğunlaştı; 2024'te ODNI OSINT Strategy, CAI Policy Framework ve AB AI Act dönüm noktaları oluştu; 2025-2026'da ise kaynak gösterme standartları, Paragon Graphite ve KVKK'nin üretken AI rehberleri gibi yeni yönetişim katmanları eklendi. [10] Aşağıdaki araç ve platform matrisi, EPIC boyunca en çok karşılaşılacak teknik katmanları,

örnek ürünleri ve bunların temel sınırlılıklarını özetler. Tablo, “araç öğretimi” yerine “görev-uygun araç seçimi” mantığını öne çıkarır.

Kuramsal ve Operasyonel Çekirdek bölüm1 — Kuram, tarih ve epistemoloji. Tanım ve kapsam açısından bu sprint, istihbaratı yalnızca bilginin toplanması değil, karar alıcı için belirsizliğin yönetimi ve anlam üretimi olarak ele almalıdır. Kapsam; istihbaratın tarihsel evrimini, “bilgi–kanıt–yorum–karar” zincirini, istihbarat çalışmalarının disiplinleşmesini ve Türkiye’de alanın kurumsal konumunu içerir. Temel kavramlar; epistemik belirsizlik, sinyal-gürültü ayrımı, sürpriz/saptama dengesi, disiplinlerarası istihbarat çalışmaları ve istihbaratın bilgi sosyolojisidir. Otoritatif eksen için UK’nin JDP 2-00 doktrini ve Türkiye’de istihbarat çalışmalarının seyrini tartışan MİA 2025 raporu birlikte okunmalıdır; OSINT’in tarihsel yükselişini ve “devrim mi evrim mi” tartışmasını güncelleyen yeni akademik hat da bu modüle dahildir. [20] 2020-2026 döneminde bu sprintin ana gelişmesi, “istihbarat = gizli kaynak” varsayımının aşınmasıdır. ODNI’nin 2024-2026 OSINT stratejisi açık ve ticari veriyi kurumsal istihbaratın merkezine taşımış; 2026 AI Index ise AI benimsemesinin, yönetişim hazırlığından daha hızlı ilerlediğini göstermiştir. Ukrayna savaşı ve ticari görüntü ekosistemi de, kamusal şeffaflığın savaş alanını “yarı saydam” hale getirdiği yeni epistemik ortamın en güçlü vaka çalışmasıdır.

Pratik tradecraft tarafında öğrencinin ilk kazanımı; her iddiayı kaynak, yöntem ve güven derecesiyle birlikte sunmayı öğrenmektir. Etik-politika cephesinde en büyük risk, veri bolluğunun güvenilirlik yanılsaması üretmesidir. Türkiye için temel boşluk, istihbarat teorisini güvenlik pratiğinden koparmadan öğreten disiplinlerarası programların sayıca az olmasıdır. bölümmodülü için önerilen teslimat, “istihbarat nedir?” sorusuna Türkiye odaklı 1.500 kelimelik kavramsal not; öğrenme hedefi ise epistemik sınırları ve kurum-misyon bağını ayırt edebilme; değerlendirme ise kısa deneme, sözlü briefing ve kaynak kalitesi rubriği olmalıdır. [21] bölüm2 — İstihbarat çevrimi, gereksinim yönetimi ve uyarı. Bu sprintin kapsamı; gereksinim formülasyonu, koleksiyon yönetimi, disiplinler arası cueing, erken uyarı, collection-to-analysis geçişi ve karar vericiyle geri-besleme hattıdır. Teorik çerçeveler; intelligence cycle, requirement management, indicator-and-warning yaklaşımı ve görev-temelli koleksiyon mimarisidir.

Güncel kaynaklar arasında JDP 2-00, warning intelligence eğitimine dair akademik çalışma ve ODNI'nin CAI yönetişim çerçevesi özellikle önemlidir; çünkü koleksiyon artık yalnızca sensör ve insan kaynağı değil, aynı zamanda ticari veri tedarik zinciri yönetimi meselesidir.

[22] 2024 sonrası gelişmeler, bu sprinti klasik çevrim anlatısının ötesine taşımıştır. ODNI'nin OSINT stratejisi ve CAI policy framework'ü, gereksinim yönetimini açık/ticari veri pazarlarıyla doğrudan ilişkilendirirken, yeni kaynaklandırma standartları ürünlerin izlenebilirliğini artırmıştır. Pratik tradecraft tarafında öncelik; PIR/IR üretimi, göstergeler tablosu, collection plan, cross-cueing ve "uyarı eşikleri" tasarlamaktır. Etik ve politika açısından risk, özellikle hassas ticari veri kullanımında mission creep ve amaç sapmasıdır. Türkiye için öneri, USOM, savunma, kolluk, diplomasi ve afet yönetimi arasında ortak bir gereksinim ontolojisi oluşturulmasıdır. bölümçıktısı olarak öğrenciden bir "uyarı panosu" ve koleksiyon planı istenmeli; öğrenme hedefi, gereksinim ile veri tedariki arasındaki farkı görebilmek olmalı; değerlendirme de zaman baskısı altında senaryo-temelli kriz hücre çalışmasıyla yapılmalıdır. [23] bölüm3 Analitik tradecraft ve yapılandırılmış yöntemler. Bu sprint, istihbarat analizinin teknik değil muhakeme işi olduğunu öğretmelidir. Kapsam; yapılandırılmış analitik teknikler, alternatif hipotezler, gösterge matrisi, kırmızı takım, kalibrasyon, belirsizlik dili, argüman haritalama ve kaynaklandırılmış analitik yazımdır.

Güncel literatür, analist eğitiminde vaka-temelli, ürün-temelli ve sürpriz azaltmaya odaklı yöntemlerin önemini vurgular; OSINT ve AI kaynaklarının artışı ise izlenebilirlik ve kaynak disiplini ihtiyacını büyütür. [24] 2020-2026 döneminde bu sprintin yeni boyutu, AI destekli analizin "**hız–doğruluk–denetlenebilirlik**" üçgenini gerilimli hale getirmesidir. NIST AI RMF ve üretken AI profili, analitik çıktılar için güvenilirlik, gözetim, ölçme ve yönetme mantığını öne çıkarır. Pratik tradecraft için önerilen yöntem, her analitik ürünün en az üç katmandan oluşmasıdır: hipotez seti, kanıt matrisi ve güven seviyesi. Etik boyutta iki risk öne çıkar: otomasyon yanlılığı ve kaynakların görünürde çoğalmasına rağmen doğrulanabilir kanıtın azalması. Türkiye için en önemli boşluk, kurumlar arası ortak analitik yazım standardı ve hata-sonrası öğrenme kültürüdür. Modül teslimatı için iki rakip hipotezi karşılaştıran kısa intelligence note; öğrenme hedefi için belirsizliği nicel

olmadan ama disiplinli biçimde ifade etme; değerlendirme için de akran denetimi, kaynak izi kontrolü ve sözlü savunma önerilir. [25] bölüm4 — **HUMINT,** karşı-istihbarat ve insider threat.

Tanım ve kapsam bakımından bu sprint; insan kaynaklı bilgi toplama, debriefing, source validation, liaison, counterintelligence ve içeriden tehdidin kurumsal güvenlikteki yerine odaklanmalıdır. Resmî ve otoritatif eksende FM 2-22.3 HUMINT Collector Operations, FBI'ın karşı-istihbarat çerçevesi, DNI/NCSC insider threat yapıları ve 2024 tarihli DoD Insider Threat Program talimatı temel alınmalıdır. Bu kaynaklar, HUMINT'in yalnızca sorgu veya ajan ağı değil, aynı zamanda kurum güvenliği, kaynak koruma ve davranışsal risk tespit kapasitesi olduğunu gösterir. [26] Yakın dönem gelişmelerinde iki eğilim dikkat çekmektedir:

Birincisi içeriden tehdidin artık yalnızca fiziksel sızma değil veri, ağ ve süreç bilgisine dayalı karmaşık risk olarak görülmesi;

İkincisi HUMINT eğitiminin dil, kültür ve güven ilişkisine daha fazla yatırım yapmasıdır. 2025'te modernize edilmiş sorgulama/dil eğitimi tartışmaları ve Reuters/AP tarafından raporlanan örnek olaylar ,örneğin hassas askeri veriyi Rusya'ya aktarmaya çalışan U.S. Army personeli ve eski FBI karşı-istihbarat yetkilisi **McGonigal vakası** , içeriden tehdit ile etik erozyon arasındaki bağlantıyı görünür kılmıştır.

Pratik tradecraft; rapport-based elicitation, kaynak güvenilirlik derecelendirmesi, çoklu doğrulama, pattern-of-life çapraz kontrolü ve insider risk göstergeleri etrafında kurulmalıdır. Etik ve hukuk açısından işkence yasağı, orantılı personel gözetimi ve masumiyet karinesi temel sınırlardır. Türkiye için öneri, savunma sanayii ekosistemi, kritik altyapılar ve kamu kurumlarında ortak insider threat mimarisinin **HUMINT/CI** ve siber güvenlik birimleriyle entegre edilmesidir. Modül teslimatı olarak bir kaynak değerlendirme dosyası ve insider threat playbook taslağı; öğrenme hedefi olarak insan kaynağından gelen bilginin kırılganlığını anlama; değerlendirme olarak da rol canlandırma, vaka çözümleri ve etik değerlendirme notu önerilir. [27] Açık Kaynak ve Coğrafi İstihbarat bölüm5 — **OSINT, SOCMINT** ve **PAI/CAI** ekosistemi. Bu sprintin tanımı, **OSINT**'i "internet taraması" düzeyine indirmeden; kamusal ve ticari veri, kaynak gösterme, doğrulama ve üretim disiplini olan ayrı bir istihbarat alanı olarak öğretmektir.

Kavramsal çerçeveler; PAI/CAI ayrımı, açık kaynak çevrimi, source grading, zincirleme doğrulama, çevrim içi ağ izleri ve dijital saha araştırmasıdır.

Bugünün en önemli birincil kaynakları ODNI IC OSINT Strategy 2024-2026, DoD'nin PAI direktifi, ODNI'nin CAI framework'ü ve Aralık 2024 standardı etrafında gelişen kaynaklandırma disiplini olup, Türkçe eksende MİA'nın modern savunma istihbaratı ve OSINT yaklaşımı analizi özellikle değerlidir. Bu kombinasyon, OSINT'in artık "yardımcı" değil profesyonelleştirilmiş bir ana kabiliyet olduğunu açık biçimde göstermektedir. [28] 2020-2026 arasındaki en önemli değişim, ticari veriyle kamuya açık verinin birbirine eklemlenmesi ve bunun mahremiyet etkileridir. ODNI çerçevesi, hassas CAI erişiminde belgeleme ve iki yılda bir kamuya raporlama yükümlülüğü getirirken, Türkiye'de MİA ve istihbarat çalışmaları literatürü bu alanda kurumsal profesyonelleşme ve metot standartlarının henüz gelişme aşamasında olduğuna işaret eder. Tradecraft bakımından bu sprintte öğretilmesi gereken çekirdek pratikler; geolocation, chronolocation, platform metadata okuması, sosyal ağ haritalama, alan adı ve altyapı iz sürme, ters görsel arama mantığı ve kaynak izi tutma disiplinidir.

Shodan gibi araçlar dış yüzey keşfi için, platform şeffaflık merkezleri etki operasyonları için ve doğrulanmış kurumsal raporlar da referans OSINT üretimi için kullanılabilir; ancak bunların hiçbiri saha doğrulaması ve metodolojik şüpheciliğin yerini tutmaz. Etik-politika boyutunda temel mesele, kişisel veri, ticari veri ve meşru araştırma arasındaki sınırların netleştirilmesidir. Türkiye için öneri; Türkçe, Arapça, Rusça, Farsça ve bölgesel lehçeleri içeren çok dilli OSINT laboratuvarı ile ortak kaynaklandırma standardı geliştirilmesidir. Modül teslimatı için tam kaynaklanmış bir OSINT dosyası; öğrenme hedefi için "doğru görünene değil, doğrulanabilene inanma" disiplini; değerlendirme için logbook, metod notu ve canlı doğrulama tatbikatı uygundur. [29] bölüm6 — GEOINT, IMINT ve ticari görüntü istihbaratı. Tanım ve kapsam bakımından bu sprint, görüntü ve coğrafi verinin yalnızca harita üretmek için değil, fiziksel özellikleri ve coğrafi olarak referanslanmış faaliyetleri tasvir, değerlendirme ve görselleştirme için kullanıldığını öğretmelidir. NGA'nın tanımı, GEOINT'i açık biçimde ulusal güvenlik karar desteği olarak konumlandırır.

Temel kuramsal çerçeveler; geospatial reasoning, multi-int fusion, değişim tespiti, multispektral analiz, olay sonrası hasar değerlendirmesi ve mekânsal kanıtlamadır. Birincil literatür tarafında NGA, ESA/Copernicus, Sentinel Hub ve USGS/Landsat ekosistemi bu alanın vazgeçilmez kaynaklarıdır. [30] Yakın dönem gelişmeleri, GEOINT'in öğretiminde "ticari platform bağımlılığı" başlığını zorunlu hale getirmiştir. Planet, Ukrayna savaşını tarihin en çok belgelenen işgali olarak sunarken, Conflict Observatory ticari görüntü ve açık kaynak yöntemlerini savaş suçları belgelendirmesi için kullandı. Copernicus EMS ve EFFIS de afet ve yangın gözetiminde Avrupa ölçeğinde operasyonel bir coğrafi erken uyarı modeli oluşturdu. Buna karşılık 2025'te Ukrayna'nın GEGD/Maxar erişiminin geçici askıya alınması, ticari görüntü erişiminin jeopolitik baskı aracına dönüşebileceğini gösterdi. Tradecraft boyutunda öğrencinin AOI belirleme, çok zamanlı analiz, ground-truthing, açık kaynaklarla çapraz doğrulama ve haritalı rapor yazımını öğrenmesi gerekir. Etik ve hukuk bakımından lisans, uydu verisinin adli kanıt olarak kullanımı, sivillerin mahremiyeti ve çatışmalarda açık kaynak kanıtın zincirleme saklanması kritik başlıklardır.

Türkiye için öneri, orman yangını, sınır güvenliği, deniz yetki alanları ve kritik altyapı gözetimini tek çatı altında birleştiren yerli analiz kapasitesinin ve tedarik çeşitliliğinin artırılmasıdır. Modül teslimatı olarak haritalı bir change-detection raporu; öğrenme hedefi olarak görüntü okuryazarlığı; değerlendirme için de zaman damgalı ekran kayıtları, veri iş akışı notu ve kısa sözlü sunum önerilir. [31] Siber Tehdit ve Yapay Zekâ bölüm7 — Siber tehdit istihbaratı, detection engineering ve adli bilişim. Bu sprint, siber güvenliği teknik savunmadan ayırarak istihbarat mantığıyla öğretmelidir. Kapsam; tehdit aktörü profilleme, TTP modelleme, olay zenginleştirme, IOC/IOA paylaşımı, detection-as-code, tehdit avcılığı ve adli bilişimle CTI arasındaki geri-besleme çevrimini içerir. Temel kurumsal çerçeveler MITRE ATT&CK, STIX/TAXII ve MISP mimarisidir; Sigma detection kuralları, VirusTotal ve Shodan gibi platformlar da operasyonel yardımcı katmanları temsil eder. Bu alanın state of the art'ı, standardize edilmiş veri biçimleriyle makinece işlenebilir, ATT&CK'e haritalı ve detection mühendisliğiyle kapanan bir CTI hattıdır. [32] 2023-2026 döneminin ana vaka hattı Çin bağlantılı Volt Typhoon ve Salt Typhoon kampanyalarıdır.

CISA/NSA ortak uyarıları, Volt Typhoon'un kritik altyapıda "living off the land" teknikleriyle uzun süreli kalıcılık kurduğunu; 2025 duyuruları ise Salt Typhoon'un küresel telekom ağlarını besleyen bir casusluk sistemi için kullanıldığını ortaya koydu. 2025 Reuters haberi, bir U.S. National Guard ağının kapsamlı şekilde ihlal edildiğini raporladı; bu da yerel-federal-sivil füzyon düğümlerinin yeni zafiyet alanları olduğunu gösterdi. Pratik tradecraft için önerilen hat, ATT&CK haritalama, STIX/TAXII üzerinden paylaşım, MISP korelasyonu, Sigma ile kural üretimi ve olay sonrası adli çıkarımların CTI veri tabanlarına geri beslenmesidir. Etik ve hukuk bakımından pasif keşif ile yetkisiz müdahale arasındaki sınır, PII içeren telemetri paylaşımı ve özel sektörle istihbarat değişimi dikkatle yönetilmelidir. Türkiye için öneri, USOM/SOME ağı üzerine sektör bazlı paylaşım toplulukları, ATT&CK kapsama haritaları ve asgari STIX/TAXII birlikte işlerliğinin inşa edilmesidir. Modül teslimatı için ATT&CK'e haritalı CTI raporu; öğrenme hedefi olarak TTP'den savunma kararı türetebilme; değerlendirme için ise tabletop olay yönetimi ve detection gap analizi uygundur. [33] bölüm8 — Yapay zekâ destekli istihbarat, otomasyon ve gözetim teknolojileri.

Bu sprintin tanımı, AI'ı ne sihirli çözüm ne de salt tehdit olarak görmek yerine; istihbarat iş akışlarını dönüştüren ama yoğun risk yönetişimi gerektiren bir katman olarak öğretmektir. Kapsam; NLP destekli özetleme, varlık eşleme, görüntü/video analizi, anomali saptama, model denetimi, sentetik medya tespiti, otomasyon yanlılığı ve mercenary spyware ekonomisini içerir. Otoritatif çerçeveler NIST AI RMF, NIST üretken AI profili ve AB AI Act'tir. Türkçe tarafta MİA'nın yapay zekâ-toplum-güvenlik ve yapay zekâ çağında siber güvenlik raporları, Türkiye bağlamı için güçlü birer başlangıç kaynağıdır. [34] 2020-2026 arasındaki en kritik gelişme, faydalı otomasyon ile ileri gözetimin aynı teknik ekosistem içinde büyümesidir. Apple'ın 2025 tehditle ilgili bildirimleri, mercenary spyware saldırılarının yüksek riskli kullanıcıları hedef almaya devam ettiğini gösterdi. U.S. Treasury'nin Intellexa yaptırımları, Predator ekosisteminin ulusal güvenlik ve insan hakları bakımından ne kadar problemli hale geldiğini ortaya koydu. Citizen Lab'in 2023 Predator doğrulaması, 2025 Paragon Graphite bulguları ve 2026 Webloc raporu, bugün yalnızca cihazın ele geçirilmesinin değil,

reklam ekosisteminden türetilmiş konum verisiyle de kitlesel gözetim yapılabildiğini gösteriyor.

Tradecraft açısından AI kullanımında altın standart, human-in-the-loop denetimi, model kartı/risk günlüğü, prompt ve veri girişlerinde OPSEC, sentetik içerik doğrulaması ve görev sonrası performans ölçümüdür. Etik ve hukuk boyutunda KVKK tavsiyeleri, mahremiyet etki değerlendirmesi, tasarımdan itibaren veri koruma ve anonimleştirme tercihlerini öne çıkarır; AB AI Act ise 2 Ağustos 2026'ya ilerleyen takvimle risk temelli uyum baskısı yaratır. Türkiye için öneri, Türkçe ve bölge dilleri için bağımsız benchmark setleri, model değerlendirme laboratuvarı ve mercenary spyware/derin sahte analiz merkezi kurulmasıdır. Modül teslimatı olarak bir "AI kullanım ve risk protokolü"; öğrenme hedefi olarak faydalı otomasyon ile riskli otomasyon arasındaki çizgiyi ayırmak; değerlendirme için de model audit notu, vaka analizi ve etik komite sunumu uygundur. [35] Etki Operasyonları ve Yönetişim bölüm9 — Etki operasyonları, propaganda algoritmaları ve sentetik medya. Bu sprint, propaganda çalışmalarını klasik psikolojik harekât anlatısından çıkarıp platform mimarisi, öneri algoritmaları, koordineli sahte davranış, bot/ağ tasarımı ve sentetik içerik ekonomisiyle birlikte ele almalıdır.

Temel çerçeveler; CIB/covert influence operations, recommender systems, platform governance, bilgi bütünlüğü ve seçim dönemi risk analizidir. Birincil kaynaklar arasında AB'nin DSA çerçevesi ile Meta, Google TAG ve TikTok'un etkide bulunma operasyonlarına ilişkin şeffaflık raporları yer alır. Bunlar, etki operasyonlarının "içerik problemi" olmaktan çok "ağ + dağıtım + görünürlük + hedefleme" problemi olduğunu göstermektedir. [36] 2020-2026 döneminde akademik literatür de aynı yönde olgunlaşmıştır. PNAS ve PNAS Nexus çalışmalarında yankı odaları, YouTube öneri sistemlerinin partizan içerik tüketimi üzerindeki etkisi ve Twitter'ın etkileşim odaklı sıralamasının bölücü içeriği daha fazla büyütebildiği gösterilmiştir. UNESCO ile Alan Turing/CETaS hattı ise seçim güvenliği bağlamında üretken AI ve etkide bulunma operasyonlarını yeni bir risk alanı olarak tartışmaktadır. Vaka tarafında 2024'te TikTok'un Rus devlet medyasıyla bağlantılı hesapları covert influence operasyonları nedeniyle kaldırması, 2025'te Google TAG ve Meta'nın İran, Çin ve Romanya bağlantılı ağları

raporlaması ve Avrupa Komisyonu'nun X'in öneri sistemine ilişkin ek bilgi talep etmesi belirleyici olaylardır.

Tradecraft boyutunda bu sprintte; anlatı haritalama, ağ topolojisi analizi, anormal büyüme tespiti, platform arası çapraz yayılım incelemesi, prebunking/inokülasyon ve içerik-provenans sinyallerinin okunması öğretilmelidir. Etik ve hukuk bakımından burada denge noktası, ifade özgürlüğünü zedelemeden şeffaflık, hesap verebilirlik ve kullanıcı kontrolünü artırmaktır. Türkiye için öneri, stratejik iletişim birimleri ile OSINT, veri bilimi ve hukuk ekiplerini ortak "information integrity" hücresinde birleştirmektir. Modül ürünleri; ağ/narrative haritası ve etki operasyonu tespit notudur; değerlendirme de veri seti temelli kısa araştırma ve platform politika özetiyle yapılmalıdır. [37] bölüm10 — Hukuk, etik, denetim ve kurumsal tasarım. Bu sprint, tüm EPIC'in normatif omurgasıdır. Kapsam; kişisel veri hukuku, istihbarat yetkisi, internet düzenlemesi, kolluk yetkileri, AI yönetişimi, gözetim teknolojileri denetimi, veri saklama ve şeffaflık ilkelerini içerir. Türkiye tarafında 2937 sayılı MİT Kanunu, 6698 sayılı KVKK ve 2024 değişiklikleri, 5651 sayılı Kanun, BTK'nın bilişim hukuku çerçevesi ve 2559 sayılı PVSK temel kamu hukuku zeminini oluşturur. Strateji düzeyinde 2024-2028 Ulusal Siber Güvenlik Stratejisi ile UYZS 2021-2025 de yumuşak yönetişim katmanları sağlar.

[38] 2023 sonrası Avrupa'daki spyware tartışmaları ve PEGA raporu, demokratik sistemlerde bile "ulusal güvenlik" gerekçesinin denetim boşlukları yaratabildiğini göstermiştir. KVKK'nin generative AI rehberleri, deepfake bilgi notu ve 2025 sempozyumları ise Türkiye'de veri koruma kuruluşunun AI/gözetim eksenine daha sistemli girdiğini gösteren önemli işaretlerdir. ODNI'nin CAI framework'ü de, ticari veri alımlarında belgelemeyi ve kamu raporlamasını zorunlu kılarak benzer bir yönetişim mantığı sunar. Bu sprintte pratik tradecraft olarak öğretilmesi gereken ana araç, "hukuki-etik etki matrisi"dir: hangi veri hangi amaçla, hangi yetkiye, hangi süreyle, hangi audit iziyle işlenecek? Türkiye için boşluk, müşterek kurumlar arası denetim, procurement governance, mahremiyet etki değerlendirmesi ve gözetim teknolojileri için bağımsız teknik inceleme kapasitesidir. Modül teslimatı olarak kısa politika notu ve etik inceleme raporu; öğrenme hedefi olarak yetki, orantılılık ve hesap verebilirlik testini

uygulayabilme; değerlendirme için de kurgusal bir tedarik dosyasının hukuk-etik incelemesi önerilir. [39] Türkiye bağlamında kullanılabilecek temel hukuk ve politika çerçevesi aşağıda karşılaştırmalı olarak özetlenmiştir:

Türkiye ve Stratejik Mimari Sentez düzeyinde bakıldığında, bu EPIC'in on sprinti altı ana bağımlılık üretir. Birincisi, kuram ve epistemoloji olmadan dijital bolluğu anlamlı bilgiye çevirmek mümkün değildir. İkincisi, çevrim ve analitik tradecraft kurulmadan OSINT/GEOINT/CTI/AI katmanları veri çöplüğüne dönüşür. Üçüncüsü, HUMINT/CI ve insider threat hattı olmadan teknik istihbarat insan unsuruna bağlanamaz. Dördüncüsü, AI ve gözetim teknolojileri ancak hukuk-etki denetimiyle birlikte kullanılabilir. Beşincisi, etki operasyonları analizi sadece içerik değil, dağıtım mimarisi ve algoritmik teşvikleri anlamayı gerektirir. Altıncısı, bunların tümü ancak ortak veri standardı, kaynaklandırma kültürü, kurumsal denetim ve eğitim boru hattıyla sürdürülebilir hale gelir. Bu mantık, ODNI'nin OSINT/CAI yaklaşımı, NIST'in risk temelli AI yönetişimi, DSA'nın şeffaflık yükümlülükleri ve Türkiye'nin siber/AI strateji belgeleri arasında kuvvetli bir uyum alanı olduğunu gösterir. [46] Türkiye açısından mevcut başlangıç noktası zayıf değildir. UYZS 2021-2025, Ulusal Siber Güvenlik Stratejisi 2024-2028, USOM altyapısı, KVKK'nin AI ve deepfake rehberleri ve MİA'nin 2025-2026 yayınları ciddi bir kurumsal farkındalık seti üretmiştir.

Buna rağmen açık boşluklar da görünmektedir: kamusal bir OSINT/PAI/CAI doktrini yoktur; sektörler arası CTI paylaşımı için STIX/TAXII/MISP tabanlı birlikte işlerlik sınırlıdır; GEOINT'te ticari tedarik bağımlılığına karşı yedekleme stratejisi net değildir; Türkçe ve bölgesel diller için güvenilir benchmark ve veri kümeleri yetersizdir; istihbarat çalışmaları eğitimi henüz ülke çapında standartlaşmış değildir; gözetim teknolojileri ve AI kullanımında müşterek hukuk-etik audit kurulları kurumsallaşmamıştır. MİA'nin "Türkiye'de İstihbarat Çalışmaları" raporu, alanın geliştiğini ancak daha sistemli bir akademik-profesyonel mimariye ihtiyaç bulunduğunu açıkça ima etmektedir. [5] Bu nedenle önerilen stratejik mimari, "merkezî tek mega-kurum" modelinden çok, ortak standartlara dayalı müşterek ağ modeli olmalıdır. Politika düzeyinde ilk adım, Türkiye'ye özgü bir açık/ticari veri istihbaratı doktrininin yayımlanmasıdır. Bu doktrin, ODNI'nin CAI framework'ündeki belgeleme mantığını ve KVKK'nin mahremiyet etki

değerlendirmesi yaklaşımını uyarlayarak; hangi kurumun hangi veri türüne, hangi yetkiyle, hangi audit iziyle erişeceğini tanımlamalıdır.

Kurumsal düzeyde ikinci adım, MİA ekseninde ama BTK, KVKK, USOM, TÜBİTAK BİLGEM, savunma kurumları, kolluk ve üniversiteleri kapsayan bir "İstihbarat Çalışmaları ve Analitik Mesleki Yeterlilik Ağı" kurulmasıdır. Teknoloji düzeyinde üçüncü adım, çok dilli veri kürasyonu, görüntü anotasyonu, CTI paylaşım standartları, sentetik medya test laboratuvarları ve AI model değerlendirme setleri için ulusal müşterek altyapıdır. [47] Aşağıdaki yol haritası, önerilen yapının uygulanabilir bir eylem planına dönüştürülmüş halidir:

EPIC'in eğitim tasarımı açısından önerilen müfredat akışı da aşağıdaki gibidir. Bu akış, önce analitik temeli kurar; sonra disiplinleri ekler; en sonda yönetişim ve Türkiye'ye özgü capstone katmanına geçer. Eğitim süresi belirtilmediği için üç seçenek makuldür: hızlı program için 10 x 3 saat; profesyonel sertifika için 10 x 12 saat; lisansüstü seminer için 14 hafta + capstone. Uyarı zekâsı ve analitik eğitim literatürü, ürün-temelli ve senaryo-temelli değerlendirmenin yalnız sınavdan daha etkili olduğunu düşündürmektedir. [48] Önerilen değerlendirme mimarisi, her sprintte küçük ama izlenebilir ürünler; program sonunda ise birleşik capstone kullanılmasını gerektirir. Bu capstone'un ideal biçimi, Türkiye'ye odaklı çok kaynaklı bir stratejik uyarı dosyasıdır: kısa istihbarat notu, kaynaklandırma ekleri, haritalı GEOINT parçası, ATT&CK haritası, AI risk notu, etki operasyonu ağ analizi ve hukuk-etik inceleme eki. Böyle bir capstone, istihbarat ürününün sadece "doğru" değil, aynı zamanda yeniden üretilebilir, savunulabilir ve denetlenebilir olması gerektiğini öğretir. Bu da "İstihbarat Teorisi 2026" başlığının en kritik dersi olur: 2026'da iyi istihbarat; çok kaynaklı, analitik olarak disiplinli, teknik olarak izlenebilir ve hukuken savunulabilir olandır.

[49] İlgili alanlarda 2024-2026 dönemine dair seçilmiş güncel gelişmeler için şu haber kaynakları da yararlıdır:
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf [3] [30]
https://www.nga.mil/about/About_Us.html
https://www.nga.mil/about/About_Us.html [4] [34] https://digital-

strategy.ec.europa.eu/en/policies/regulatory-framework-ai https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai [5] [44] https://hgm.uab.gov.tr/duyurular/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2024-2028-yayimlandi https://hgm.uab.gov.tr/duyurular/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2024-2028-yayimlandi [7] [24] [25] [48] https://gsis.scholasticahq.com/article/27802-strategic-warning-and-anticipating-surprise-assessing-the-education-and-training-of-intelligence-analysts.pdf https://gsis.scholasticahq.com/article/27802-strategic-warning-and-anticipating-surprise-assessing-the-education-and-training-of-intelligence-analysts.pdf [9] [20] [22] https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf [10] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/311518p.pdf https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/311518p.pdf [11] https://documentation.dataspace.copernicus.eu/APIs/SentinelHub.html https://documentation.dataspace.copernicus.eu/APIs/SentinelHub.html [12] https://www.usgs.gov/landsat-missions/landsat-satellite-missions https://www.usgs.gov/landsat-missions/landsat-satellite-missions [13] [31] https://www.planet.com/ukraine-photo-story/ https://www.planet.com/ukraine-photo-story/ [14] [32] https://attack.mitre.org/ https://attack.mitre.org/ [15] https://www.oasis-open.org/standard/6426/ https://www.oasis-open.org/standard/6426/ [16] https://sigmahq.io/ https://sigmahq.io/ [17] https://www.virustotal.com/ https://www.virustotal.com/ [18] https://www.shodan.io/ https://www.shodan.io/ [19] https://transparency.meta.com/metasecurity/threat-reporting/ https://transparency.meta.com/metasecurity/threat-reporting/ [26] https://www.marines.mil/Portals/1/Publications/FM%202-22.3%20%20Human%20Intelligence%20Collector%20Operations_1.pdf https://www.marines.mil/Portals/1/Publications/FM%202-22.3%20%20Human%20Intelligence%20Collector%20Operations_1.pdf [27]

https://mipb.ikn.army.mil/media/gjzfvkwh/b_modernizing_online.pdf
https://mipb.ikn.army.mil/media/gjzfvkwh/b_modernizing_online.pdf [29]
https://www.intelligence.gov/commercially-available-information
https://www.intelligence.gov/commercially-available-information [33]
https://media.defense.gov/2024/Feb/07/2003389935/-1/-1/0/CSA-PRC-Compromise-US-Critical-Infrastructure.PDF
https://media.defense.gov/2024/Feb/07/2003389935/-1/-1/0/CSA-PRC-Compromise-US-Critical-Infrastructure.PDF [35]
https://support.apple.com/en-us/102174
https://support.apple.com/en-us/102174 [36] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act https://digital-strategy.ec.europa.eu/en/policies/digital-services-act [37]
https://www.pnas.org/doi/10.1073/pnas.2023301118
https://www.pnas.org/doi/10.1073/pnas.2023301118 [38] [40]
https://www.lexpera.com.tr/mevzuat/kanunlar/devlet-istihbarat-hizmetleri-ve-milli-istihbarat-teskilati-kanunu-2937
https://www.lexpera.com.tr/mevzuat/kanunlar/devlet-istihbarat-hizmetleri-ve-milli-istihbarat-teskilati-kanunu-2937 [39]
https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA%282023%29747923_EN.pdf
https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA%282023%29747923_EN.pdf [41]
https://www.turkiye.gov.tr/bilgilendirme?konu=kvkk
https://www.turkiye.gov.tr/bilgilendirme?konu=kvkk [42]
https://www.aile.tr/uploads/chgm/uploads/pages/kanunlar/5651-sayili-internet-ortaminda-yapilan-yayinlarin-duzenlenmesi-ve-bu-yayinlar-yoluyla-islenen-suclarla-mucadele-edilmesi-hakkinda-kanun.pdf
https://www.aile.tr/uploads/chgm/uploads/pages/kanunlar/5651-sayili-internet-ortaminda-yapilan-yayinlarin-duzenlenmesi-ve-bu-yayinlar-yoluyla-islenen-suclarla-mucadele-edilmesi-hakkinda-kanun.pdf [43]
https://www.egm.gov.tr/hukukmusavirligi/2559-polis-vazife-ve-selahiyet-kanunu https://www.egm.gov.tr/hukukmusavirligi/2559-polis-vazife-ve-selahiyet-kanunu [45]
https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TR-UlusalYZStratejisi2021-2025.pdf

https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TR-UlusalYZStratejisi2021-2025.pdf [47] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf bölüm| Odak | Birincil çıktı | Baskın kaynak ailesi bölüm1 | Kuram, tarih, epistemoloji | Kavramsal çerçeve notu | Doktrin, istihbarat çalışmaları bölüm2 | Çevrim, gereksinim, uyarı | Koleksiyon/uyarı matrisi | Doktrin, warning literatürü bölüm3 | Analitik tradecraft ve yapılandırılmış yöntemler | Analitik not + alternatif hipotez tablosu | Analitik eğitim literatürü, NIST/OSINT yönetişimi bölüm4 | HUMINT, CI, insider threat | Kaynak değerlendirme dosyası | HUMINT/CI doktrini, insider threat programları bölüm5 | OSINT/SOCMINT/PAI-CAI | Kaynaklanmış OSINT dosyası | ODNI, DoD PAI, Türkçe OSINT analizleri bölüm6 | GEOINT/IMINT/ticari EO | Haritalı change-detection raporu | NGA, ESA/Copernicus, USGS, ticari EO bölüm7 | CTI ve adli bilişim | ATT&CK haritalı CTI raporu | MITRE, OASIS, CISA, MISP bölüm8 | AI, otomasyon, gözetim | Model risk ve kullanım kılavuzu | NIST, AI Act, Citizen Lab, KVKK bölüm9 | Etki operasyonları ve propaganda algoritmaları | Ağ/narrative haritası | DSA, platform şeffaflık raporları, akademik çalışmalar bölüm10 | Hukuk, etik, denetim ve tasarım | Politika notu + etik inceleme | Türkiye mevzuatı, AB/ABD yönetişim çerçeveleri Katman | Araç/platform/vendör örnekleri | Temel kullanım | Güçlü yan | Temel risk/sınırlılık | İlgili bölüm| Kaynak EO/GEOINT | Sentinel Hub / Copernicus Data Space | AOI, çok zamanlı görüntü işleme, API erişimi | Hızlı erişim, AB veri ekosistemi, ölçeklenebilirlik | Eğitim gereksinimi, lisans ve iş akışı disiplini | 6 | [11] EO/GEOINT | Landsat / EarthExplorer | Tarihsel değişim analizi, çevre ve arazi kullanımı | Uzun süreklilik, ücretsiz arşiv | Taktik çözünürlük sınırlı olabilir | 6 | [12] Ticari görüntü | Planet, Maxar/GEGD | Yüksek frekanslı çatışma/altyapı izleme | Yüksek tempo, ticari esneklik | Jeopolitik bağımlılık ve erişim kesintisi riski | 6 | [13] CTI standardı | MITRE ATT&CK | TTP modelleme, tehdit-hunting ve kapsama analizi | Ortak dil, yaygın benimsenme | “Checklist”e indirgenirse yüzeyselleşir | 7 | [14] CTI paylaşımı | STIX/TAXII, MISP | Gösterge ve olay paylaşımı | Makinece işlenebilir, topluluk temelli değişim | Veri kalitesi ve gizlilik yönetimi kritik | 7 | [15]

Tespit mühendisliği | Sigma | Platformlar arası detection rule paylaşımı | Satıcı bağımsızlığı, tekrar kullanılabilirlik | Log kalitesi ve tercüme katmanı sınırlayıcı olabilir | 7 | [16] Zararlı analiz | VirusTotal | Dosya/URL çok motorlu analiz | Hızlı triage, topluluk görünürlüğü | Yanlış pozitif, örnek paylaşımı ve OPSEC riski | 7 | [17] İnternet keşfi | Shodan | Açık servis, cihaz ve saldırı yüzeyi keşfi | Dış yüzey görünürlüğü, hızlı pasif keşif | Yetkisiz yorumlama ve etik sınırlar | 5, 7 | [18] Platform şeffaflığı | Meta Threat Reports, Google TAG, TikTok Transparency | CIB/etki operasyonu takibi | Birincil platform içgörüsü | Platform önyargısı ve dış denetim sınırlılığı | 9 | [19] Çerçeve | Temel işlev | İstihbarat/analiz için etkisi | Sınırlılık veya dikkat noktası | Kaynak 2937 sayılı MİT Kanunu | Devlet istihbaratının ve MİT'in görev/esasları | Yetki ve görev mimarisinin çekirdeği | Kamuya açık detaylar sınırlı; ikincil uygulama rejimi görünürlüğü düşük | [40] 6698 KVKK ve 2024 değişiklikleri | Kişisel veri işleme kuralları | Veri işleme, aktarma, özel nitelikli veri ve uyum | Güvenlik-istihbarat istisnalarının uygulama sınırları dikkat ister | [41] 5651 sayılı Kanun | İnternet yayınları ve erişim rejimi | İçerik kaldırma, erişim, kayıt ve platform sorumlulukları | İfade özgürlüğü ve gerekçelendirme tartışmaları | [42] 2559 PVSK | Kolluk yetkileri ve kamu düzeni | Kolluk-toplanan veri ve müdahale yetkileri | İstihbarat/kolluk ayrımı ve orantılılık sorunu | [43] Ulusal Siber Güvenlik Stratejisi 2024-2028 | Ulusal siber dayanıklılık ve iş birliği vizyonu | CTI, kritik altyapı, kurumsal koordinasyon için üst çerçeve | Uygulama ayrıntılarının bir kısmı kamuya açık değil | [44] UYZS 2021-2025 ve KVKK AI rehberleri | AI dönüşümü ve veri koruma yönetişimi | İstihbaratta AI kullanımı için yumuşak yönetişim zemini | Güvenlik alanı için daha spesifik uygulama standartlarına ihtiyaç var | [45] Zaman ufku | Politika | Kurum | Kabiliyet | Ölçülebilir çıktı Kısa vade | PAI/CAI/OSINT ve kaynaklandırma standardı yayımlansın | MİA koordinasyonunda kurumlar arası çalışma grubu kurulsun | Pilot MISP/STIX-TAXII paylaşım hattı ve Türkçe OSINT laboratuvarı açılsın | İlk müşterek kaynaklandırma rehberi, ilk ortak CTI veri akışı Orta vade | AI kullanımında mahremiyet etki değerlendirmesi ve gözetim tedarik rehberi zorunlu hale gelsin | AI-gözetim teknik inceleme kurulu ile sentetik medya inceleme laboratuvarı kurulsun | Türkçe ve bölgesel diller için benchmark setleri, GEOINT eğitim modülleri, ATT&CK kapsama haritaları üretilebilsin | Kurum bazlı audit raporları, standart eğitim sertifikaları Uzun vade | İstihbarat

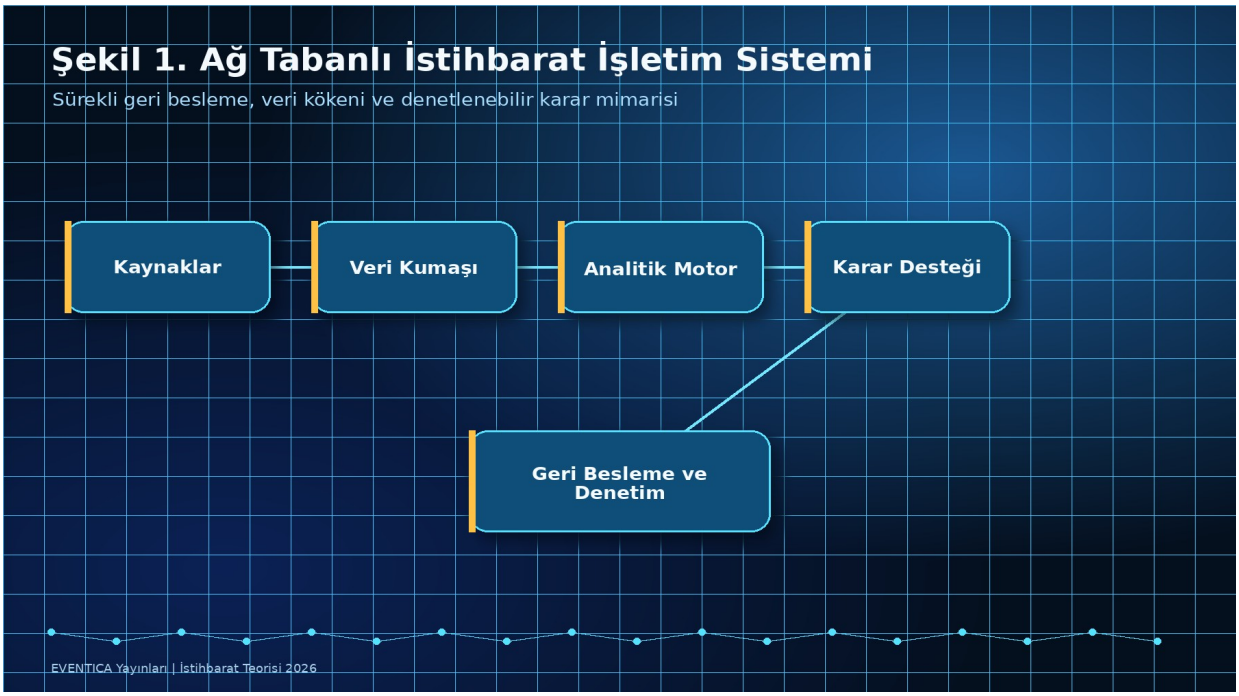
eğitimi için ulusal yeterlilik çerçevesi oluşsun | Üniversite-kamu-sanayi üçgeninde sürekli profesyonelleşme ağı kurulsun | Yerli EO analitik katmanı, model eval ekosistemi ve operasyonel platform entegrasyonu olgunlaşsın | Sertifikalı analist havuzu, kurumlar arası müşterek tatbikatlar, düzenli kamuya açık stratejik değerlendirmeler

Bölüm 1. İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp

Bu bölümün ana iddiası basit: modern istihbarat artık sadece gizli bilgi toplama meselesi değildir; insan-makine karar mimarisi, veri kumaşı ve bilişsel güvenlik meselesidir.

Tablo 3. Bölüm 1 hızlı okuma haritası

Odak	Açıklama
Ana kırılma	OODA döngüsünün lineer yorumu artık tek başına yeterli değildir.
Stratejik risk	Düşman, karar vericinin yönelim katmanını hedefleyebilir.
Savunma mantığı	Veri kökeni, sentetik içerik tespiti ve insan-makine görev paylaşımı birlikte tasarlanmalıdır.



Şekil 2. İstihbarat döngüsünün işletim sistemi mantığına evrilmesi

Tablo 4. Bilişsel harp ile klasik bilgi harekâtı ayrımı

Boyut	Klasik yaklaşım	Bilişsel harp yaklaşımı
Hedef	Bilgi ve mesaj	Algı, güven, yönelim ve

Boyut	Klasik yaklaşım	Bilişsel harp yaklaşımı
		karar mimarisi
Zaman	Kampanya bazlı	Sürekli, kümülatif ve geri bildirimli
Başarı ölçütü	Mesajın yayılması	Karar kalitesinin bozulması veya korunması
Savunma	İletişim kontrolü	Bilişsel dayanıklılık ve epistemik güvenlik

Yönetici sentezi ve ana tez

İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp Yönetici özeti Bu Bölüm mimarisinin temel savı şudur: istihbarat, artık yalnızca “gizli bilgi toplama ve analiz” faaliyeti değil, veri-kumaşı, insan-makine karar mimarisi, etki üretimi ve bilişsel güvenlikten oluşan süreğen bir sosyo-teknik işletim sistemi hâline gelmektedir. Resmî ABD savunma ve istihbarat belgeleri, klasik istihbarat döngüsünü korusa da, fiilî kurumsal yönelim “veri merkezli örgüt”, “karar üstünlüğü”, “sense–make sense–act” ve “speed and scale” eksenine kaymıştır; bu da doğrusal döngüden sürekli geri-beslemeli ağ mantığına geçiş anlamına gelir. [1] Bu dönüşümün ikinci ekseni bilişsel harptir. NATO ACT’nin güncel açıklamasında bilişsel harp, “nasıl savaştığımızın aracı” değil, “bizzat savaşın kendisi” olarak tarif edilmekte; beynin hem hedef hem de silah olduğu vurgulanmaktadır. Bunun anlamı, savaş alanının fiziksel ve enformatik boyutların ötesinde, algı, dikkat, güven, muhakeme, kimlik ve irade gibi bilişsel değişkenlere kaymasıdır. Ancak “insan zihni yeni bir operasyon alanıdır” türü daha ileri formülasyonlar NATO ekosisteminde özellikle ACT Innovation Hub metinlerinde görünse de, bunların resmî NATO doktrini değil, ACT sponsorlu keşifsel/konseptual çalışmalar olduğu bizzat metinlerde belirtilmektedir.

[2] Bu nedenle “geleneksel OODA döngüsünün çöküşü” burada literal değil, analitik bir iddia olarak kullanılmaktadır: Boyd’un modelinin kendisi değil, onun insan-merkezli, görece lineer ve kurumsal olarak içe kapalı yorumunun çöktüğü ileri sürülmektedir. Boyd’un kendi metinlerinde

OODA’nın kritik düğümü “orientation”dır; çağdaş JADC2 ve veri/AI stratejileri ise bu yönelim katmanını görünür biçimde makine hızına, veri füzyonuna ve platformlar arası bağlantıya yaslamaktadır. Aynı anda NATO, RAND ve savunma analizleri, rakibin tam da bu orientation katmanını dezenformasyon, belirsizlik, sentetik içerik ve psikolojik tekniklerle bozmayı hedeflediğini göstermektedir. Sonuç: OODA artık yalnızca “hızlandırılacak” bir döngü değildir; dış etkilerce programlanabilir, kirletilebilir, geciktirilebilir ve kısmen makineleştirilebilir bir karar ekolojisidir. [3] Tasarımsal sonuç açıktır: RAND/NATO-seviyesinde bir stratejik analitik sistem, yalnızca ISR + analitik + karar destek zinciri olarak değil; veri kökeni/provenance, sentetik içerik tespiti, hedef kitle/karar verici modelleme, insan-makine görev paylaşımı, güvenlik ve etik denetim, kamu-sivil dayanıklılık ve etkilerin ölçümünü tek bir mimaride birleştiren “bilişsel savunma işletim sistemi” olarak kurgulanmalıdır.

Bu Bölüm mimarisi, söz konusu mimarinin akademik kitap bölümü ölçeğinde nasıl inşa edileceğini detaylandırmaktadır. [4] Kapsam, kaynak tabanı ve belirsizlikler Bu metin, tam bir bölüm taslağından ziyade, yüksek yoğunluklu bir akademik bölüm mimarisi üretir. Öncelik sırası şu şekilde kurulmuştur: resmî NATO, DoD, ODNI, NIST ve ICRC metinleri; RAND ve Air University gibi birincil stratejik araştırma kurumları; ardından Türkçe akademik literatür ve savunma ekosistemi kaynakları. Türkçe literatürde özellikle “Bilgi Ortamında Harekât”, “Bilişsel Harp”, C2 fonksiyon alanı, istihbarat önyargıları ve YZ-dönüşümü etrafında kayda değer bir çerçeve oluşmaktadır. [5] Kritik metodolojik uyarı şudur: kullanıcı tarafından atıf yapılan Gemini araştırma verisi bu konuşmada sağlanmamıştır. Bu yüzden aşağıdaki on başlıkta “Bulgular” kısmı, teyitli açık kaynak/kurumsal literatüre dayanır; fakat “orijinal saha verisi”, “örnek vaka kümeleri”, “sinyal istihbaratı özetleri”, “sosyal medya anlatı kümeleri”, “ölçüm taban çizgileri” ve “karşılaştırmalı kampanya logları” için ayrı bir Gemini entegrasyon boşluğu bulunmaktadır. Bu, özellikle vaka-temelli alt-bölümlerde ampirik derinliği sınırlar.

En önemli belirsizlikler şunlardır. Birincisi, NATO çevresindeki bazı “human mind as domain” formülasyonları resmî ittifak doktrini değil, ACT/Innovation Hub niteliğinde keşifsel metinlerdir; bu yüzden bu chapter,

bunları doktrin değil stratejik söylem ve konsept evrimi olarak kullanmalıdır. İkincisi, “OODA’nın çöküşü” ifadesi literatürde standart bir kavram değildir; bu raporun sentezleyici analitik tezidir. Üçüncüsü, yapay zekânın taktik/operatif kararları tam otonomiyle güvenilir biçimde üstlenebildiğine dair kuvvetli kanıt yoktur; mevcut değerlendirmeler gözlem ve yönelim aşamalarının otomasyona daha elverişli, üst-düzey kararın ise daha kırılgan olduğunu göstermektedir. Dördüncüsü, bilişsel harp ve enformasyon operasyonlarına ilişkin uluslararası hukuk çerçevesi gelişmektedir ancak tamamlanmış değildir; IHL ve insan hakları hukuku uygulanır, fakat uygulama sınırları ve koruma boşlukları tartışmalıdır. [6] Bu nedenle aşağıdaki mimari, iki katmanlı okunmalıdır: yüksek güvenilirlikli kurumsal çekirdek ve Gemini ile doldurulacak ampirik genişleme katmanı. Bölüm yazımında bu ayrım açıkça korunmalıdır.

Kuramsal çekirdek

1. Ana tez Amaç: Bölümün merkez argümanını netleştirmek: istihbaratın ontolojik dönüşümü, nesnesi “dünya hakkında bilgi” olan bir faaliyet olmaktan çıkıp, “karar ortamını şekillendiren ve rakibin yönelimini bozmayı hedefleyen” bir yapı hâline gelmesidir. Bu çerçevede bilişsel harp, istihbaratın sonradan hizmet verdiği bir alan değil, istihbarat mimarisinin içine yerleşmiş asli bir fonksiyondur.

Metodoloji: Boyd’un OODA ve “orientation” vurgusu; JADC2’nin “sense, make sense, act” yaklaşımı; IC veri stratejileri; NATO ACT bilişsel harp tanımları; RAND’ın bilgi ortamı, psikolojik harp ve AI-stratejik risk çalışmalarının karşılaştırmalı sentezi. [7] Bulgular: Boyd’da orientation, genetik miras, kültürel gelenek, önceki deneyim ve gelişen koşulların şekillendirdiği odak noktasıdır; dolayısıyla OODA’nın en kırılgan yeri teknik sensör katmanı değil, yorumlayıcı insan/makine ara-katmanıdır. JADC2 ve DoD veri/AI stratejileri, bu ara-katmanı veri füzyonu, analitik ve AI ile hızlandırmak isterken, NATO ACT ve RAND çalışmaları rakibin tam da psikolojik/algısal düzeyde karar üstünlüğü aradığını göstermektedir. Bu yüzden “çöküş”, döngünün yok oluşu değil; tekil, insan içi ve sıralı karar çevriminin, ağsal, dış etkilerle manipüle edilebilir ve kısmen otomatikleştirilmiş karar ekosistemi karşısında yetersizleşmesidir. [8] Gemini entegrasyon boşluğu: Bu başlık altına, Gemini çıktılarından türetilmiş

özgül kampanya örnekleri, anlatı ekosistemi haritaları, karar gecikmesi ölçümleri ve sentetik medya yoğunluğu verileri yerleştirilmelidir.

Öneriler / tasarım gereksinimleri: Bölüm tezi, “istihbarat artık bilgi üretmez; yönelim, güven ve irade mimarisi üretir” cümlesi etrafında kurulmalıdır. Kavramsal olarak üç kırılma açık yazılmalıdır: doğrusal döngüden sürekli geri beslemeye geçiş; platform-merkezden veri-merkeze geçiş; düşman düzeninin bozulmasından zihinsel düzenin bozulmasına geçiş. Bu üç kırılma, bölümün sonraki bütün alt-bölümlerinin ortak aksı olmalıdır. [9]

2. Kavramsal çerçeve Amaç: Tanımlar, ontoloji, aktörler ve bilgi akışlarını tek bir çatı altında birleştirmek; Türkçe literatürdeki terminolojik karmaşayı giderirken NATO/DoD bağlamıyla uyumlu bir sözlük kurmak.

Metodoloji: Türkçe “Bilgi Ortamında Harekât” önerisini, NATO/DoD’nin information environment, OIE, cognitive warfare ve human-machine teaming literatürüyle eşleştiren katmanlı kavramsal model. Türkçe literatür, bilişsel harp ile bilgiye yönelik harp ayrımını açık biçimde savunur; bu ayrım burada korunmaktadır. [10] Bulgular: En uygun ontoloji dört varlık kümesi gerektirir: aktörler (devlet, istihbarat topluluğu, platform şirketleri, vekil ağlar, kitleler, kanaat önderleri); nesneler (veri, anlatı, güven, kimlik, dikkat, hukukî meşruiyet, teknik altyapı); süreçler (toplama, füzyon, anlamlandırma, etki tasarımı, dağıtım, ölçüm, adaptasyon); etkiler (algı kayması, gecikme, kutuplaşma, caydırma, aldatma, ajans kaybı, komuta zinciri bozulması). Türkçe literatürün önerdiği gibi fiziksel, sanal ve bilişsel alt-boyutları aynı bilgi ortamı içinde düşünmek analitik olarak daha doğrudur; çünkü teknik saldırı ile bilişsel etki artık ayrı kampanyalar değil, tek bir kampanya yığınının katmanlarıdır. [11] Gemini entegrasyon boşluğu: Gemini veri setleri varsa burada taksonomiye bağlanacak örnek düğümler tanımlanmalıdır: anlatı kümeleri, botnet davranış paternleri, platformlar arası yayılım zincirleri, hedef kitle segmentasyonları, psikografik vektörler.

Öneriler / tasarım gereksinimleri: Kavramsal çerçevede terminoloji şu sırayla sabitlenmelidir: en üstte Bilgi Ortamında Harekât; bunun altında Bilgiye Yönelik Harp ve Bilişsel Harp; onların altında siber, elektronik harp, MISO/PSYOP, dezenformasyon, influence ops, lawfare, data exploitation ve adversarial AI alt-kümeleri. “İnsan zihni savaş alanıdır” ifadesi

kullanılacaksa, resmî NATO doktrini şeklinde değil, ACT/NATO çevresindeki gelişen stratejik söylem olarak dikkatli çerçevelenmelidir. [12] Aşağıdaki akış, bu ontolojik kaymayı bölümün ana şeması olarak verebilir:

Bu şema, Boyd'un orientation merkezliliği, JADC2'nin sense–make sense–act mantığı, IC veri yaşam döngüsü ve Zero Trust/AI güvenlik mimarilerinin sentezidir. [13] Mimari ve mekanizmalar

3. Sistem mimarisi Amaç: Bileşenler, veri katmanları, kontrol döngüleri ve insan-makine arayüzlerini tasarlamak; klasik istihbarat yapısından bilişsel harp mimarisine geçişi karşılaştırmalı olarak göstermek.

Metodoloji: DoD veri-merkezli dönüşüm, JADC2, IC Data Strategy, OSINT 2024–2026, Zero Trust referans mimarisi, NIST AI RMF ve DoD RAI ilkeleri bir araya getirilmiştir. Bu, bölümün "tasarım bölümü" için normatif omurgayı sağlar. [14] Bu tablo, DoD'nin veri merkezli organizasyon, JADC2, IC veri stratejisi, OSINT orkestrasyonu, Zero Trust analitik/AI katmanı ve NIST'in sosyo-teknik risk yönetimi yaklaşımının birlikte okunmasıyla türetilmiştir. [15] Bulgular: Resmî stratejiler, bölüm mimarisinin en az sekiz modüle sahip olması gerektiğini düşündürmektedir: sensör ve toplama orkestrasyonu, veri kumaşı ve katalog, provenance/pedigree/lineage yönetişimi, senaryo ve hedef modelleme, anlatı/etki motoru, insan-makine karar hücresi, TEVV/RAI/hukuk kapısı, telemetri ve kampanya geri-besleme katmanı. IC veri yaşam döngüsü analiz ve sömürüm aşamasında veri değerinin hedefli sorgular, analitik modeller ve otomatik analitik yeteneklerle üretildiğini; aynı anda köken, soy ağacı ve zincirin korunması gerektiğini açıkça vurgular. Bu, bilişsel harp mimarisinde "hakikat zinciri"nin teknik karşılığıdır. [16] Gemini entegrasyon boşluğu: Burada sistem gereksinimlerini sahaya bağlayacak özgül bileşenler eklenmelidir: hangi dil modelleri, hangi anlatı ontolojisi, hangi veri gölleri, hangi platform konektörleri, hangi teyit motorları, hangi kırmızı takım senaryoları.

Öneriler / tasarım gereksinimleri: Bölümde önerilen referans mimari, "product-centric intelligence" yerine data-centric cognitive security stack olarak adlandırılmalıdır. İnsan-makine arayüzlerinde üç zorunlu alan bulunmalıdır: güven puanı ve belirsizlik sunumu; karşı-anlatı/senaryo seçenekleri; otomasyonun durdurulması ya da geri alınması için governable kill-switch mantığı. [17]

4. Mekanizma analizi Amaç: Etkileşimler, geri besleme döngüleri ve manipülasyon tekniklerini ampirik mekanizma düzeyinde çözümlemek.

Metodoloji: RAND'ın influence operations ve information environment çalışmaları; RAND'ın deepfakes, microtargeting, ML-driven programs ve spoofing vurgusu; NATO'nun bilişsel harp ve kamu güveni erozyonu tespitleri; ICRC'nin ajans ve siviller üzerindeki etkiler değerlendirmesi üzerinden mekanizma tablosu çıkarılmıştır. [18] Bulgular: Bilişsel harp mekanizması beş birleşik çevrimden oluşur: algısal kirletme (sahte/yarı-doğru/sentetik girdi ile gözlem katmanını kirletme), yönelim bozma (belirsizlik, aşırı veri, çelişkili anlatı, sahte kesinlik), karar geciktirme (komuta kademelerinde dikkat ve güven maliyeti yaratma), davranış yönlendirme (mikro-hedefleme, çerçeveleme, yankı odası, sosyal kanıt üretimi) ve geri-beslemeli pekiştirme (telemetri ile modelin yeniden ayarlanması). RAND, stratejik caydırıcılığın bilgi manipülasyonu yüzünden deepfake, microtargeting, ML-driven programs ve spoofing ile bozulabileceğini belirtir; NATO S&T değerlendirmeleri de generative AI ve deepfake'lerin kamu güvenini ve kurumsal meşruiyeti aşındırdığını vurgular. [19] Gemini entegrasyon boşluğu: Manipülasyon teknikleri burada platform, dil, ağ yapısı ve hedef kitle bazında ayrıştırılmalıdır. Özellikle taktik seviyede sahte alarm, operatif seviyede karar doygunluğu ve stratejik seviyede güven erozyonu için ölçüm matrisleri Gemini verisiyle doldurulmalıdır.

Öneriler / tasarım gereksinimleri: Bölüm, bilişsel harp tekniklerini yalnızca taktik hileler değil, karar mimarisi saldırıları olarak sınıflandırmalıdır. Buna göre savunma tarafında erken uyarı için üç ölçüm ailesi tanımlanmalıdır: semantik sapma göstergeleri, ağ-yayılım anomali göstergeleri ve karar zinciri sürtünme göstergeleri. Ayrıca "bilgi doğrulama" ile "yönelim doğrulama" ayrılmalı; doğru bilgi tek başına yeterli sayılmamalıdır, çünkü asıl hedef karar vericinin yorum çerçevesidir. [20]

Stratejik ve operasyonel mantık

5. Stratejik mantık Amaç: Hedefler, oyun teorisi modelleri, caydırma ve aldatmayı bilişsel harp bağlamında kurgulamak.

Metodoloji: JCS Deterrence Operations JOC'un "adversary decision calculus" yaklaşımı, RAND'ın deterrence/AI çalışmaları ve Çin'in yeni nesil psikolojik harp incelemeleri üzerinde analitik formalizasyon yapılmıştır. Burada bazı modeller doğrudan belge adı olarak değil, bu belgelerin altında önerilen analitik formelleştirme araçları olarak sunulmaktadır. [21] Bulgular: Stratejik düzeyde hedef, fiziksel imha değil rakibin karar hesabını yeniden ağırlıklandırmaktır. JOC, bunun üç yolunu açıkça verir: faydayı inkâr etmek, maliyet yüklemek ve hasmı restraint'e teşvik etmek. Bilişsel harp bu üç yolu karar vericinin algılanan fayda-maliyet hesabına müdahale ederek uygular. Buna en uygun analitik formalizasyonlar şunlardır: Bayesyen ikna / information design modeli, çünkü rakibin posterior inançlarını şekillendirmeyi hedefler; tekrarlı sinyal oyunu, çünkü stratejik iletişim ve aldatma tek atımlık değil kampanya mantığındadır; principal-agent modeli, çünkü insan-makine ekiplerinde öneri üreten model ile karar veren komutan arasında yetki ve sorumluluk ayrışır; latency/queueing oyunu, çünkü karar avantajı çoğu kez doğruluk kadar gecikme süresiyle ilgilidir. Bu teorik çerçeve, resmî belgelerde geçen "decision calculus", "information advantage", "speed of relevance" ve "manage perceptions" mantığının teknikleştirilmesidir. [22] Gemini entegrasyon boşluğu: Eğer Gemini çıktıları aktör-bazlı vaka çözümlemeleri veya kampanya logları içeriyorsa, bu modeller burada kalibre edilmelidir: hangi aktör hangi fayda/maliyet çarpanına duyarlı, hangi anlatı hangi gecikme fonksiyonunu üretiyor, hangi karşı-etki hangi eşikte caydırıcı oluyor.

Öneriler / tasarım gereksinimleri: Chapter, stratejik mantığı yalnızca "etki" değil karar hesabı mühendisliği olarak formüle etmelidir. Ayrı bir alt-kısımda "cognitive deterrence" ve "cognitive deception" ayrımı yapılmalı; biri rakibin eşiğini yükseltirken diğeri rakibin dünya modelini eğriltir. Çin bağlamında yanlış güven ve yanlış başarı algısının kriz tırmanmasını tetikleyebileceği özellikle vurgulanmalıdır. [23]

6. Operasyonel etkiler Amaç: Taktikler, istihbarat süreçleri ve karar zincirlerinin nasıl değiştiğini göstermek.

Metodoloji: OIE/IO ile istihbarat arasındaki rol gerilimlerini inceleyen RAND raporu; ODNI'nin OSINT ve veri stratejileri; ICD 203 ve ICD 206 gibi analitik/sourcing standartları; JADC2 ve mission command çerçeveleri. [24] Bulgular: Operasyonel düzeyde beş etki ortaya çıkar. Birincisi, istihbarat döngüsü kalır ama baskın işletim mantığı sürekli veri akışı ve görev sırasında yeniden yönelim olur. İkincisi, OIE için IO ve istihbarat toplulukları arasında rol ve sorumluluk çatışması büyür; RAND bunu doğrudan "greatest point of friction" olarak tanımlar. Üçüncüsü, OSINT ve commercially/publicly available information, yalnızca tamamlayıcı değil, kimi durumlarda en hassas toplama araçlarının yerine kullanılabilecek öncelikli katman olur. Dördüncüsü, analitik standartlar nesnellik, tüm kaynaklara dayalı değerlendirme, belirsizlik açıklaması ve önyargı azaltma yükümlülüğünü artırır. Beşincisi, karar zincirleri, tek merkezli komuta mantığından, görev komutası ve veri destekli kenar kararları yönünde evrilir; fakat bu, orientation dokusunun bozulması hâlinde zincirin her düzeyde kırılganlaşması demektir. [25] Gemini entegrasyon boşluğu: Saha kampanyaları, sosyal medya manipülasyonu, komuta merkezine yönelik doygunluk saldırıları, yanlış alarm üretimi ve open-source exploitation vakaları burada operasyonel vignette olarak işlenmelidir.

Öneriler / tasarım gereksinimleri: Bölüm, klasik istihbarat sürecine ek üç yeni operasyonel işlev önermelidir: narrative warning, orientation assurance, decision chain telemetry. Ayrıca analist eğitimi yalnızca ACH, Delphi ve red-team gibi tekniklerle sınırlı kalmamalı; platform mantığı, sentetik medya adli bilişimi ve insan-makine ekip çalışması modülleri eklenmelidir. Türkçe literatürde önyargı yönetimi ve C2 dönüşümü üzerine gelişen tartışma, bu öneri için güçlü bir yerel dayanak sağlar. [26]

Risk, AI dönüşümü ve güvenlik

7. Risk analizi Amaç: Teknik, etik, hukukî ve stratejik riskleri tek tabloda sınıflandırmak.

Metodoloji: NIST AI RMF ve AML taksonomisi, NIST GAI profili, DoD RAI Pathway, DoD AI siber güvenlik kılavuzu, ICD 505, ICRC hukuk tartışmaları

ve NATO AI stratejisi birlikte okunmuştur. [27] Bu risk matrisi, NIST'in AI'yi sosyo-teknik risk olarak ele alışı, AML yaşam döngüsü tehditleri, GAI'ye özgü provenance/test/incident disclosure gereksinimleri, DoD'nin RAI/TEVV ve tedarik zinciri hassasiyetleri ile ICRC'nin sivil koruma ve ajans vurgusundan türetilmiştir. [28] Bulgular: Riskler yalnızca teknik değildir; en kritik risk, teknik kusurun stratejik yanlış güven üretmesidir. RAND, AI ve özerkliğin makine hızında kararlarla caydırıcılık ve tırmanma dinamiklerini bozabileceğini; Çin üzerine yaptığı araştırmalarda ise psikolojik harp teknolojilerine duyulan aşırı güvenin kriz davranışını yanlış kalibre edebileceğini belirtir. ICRC ve hukuk literatürü, bilişsel operasyonların sivilleri doğrudan potansiyel hedef hâline getirmesinin savaş/barış ve sivil/asker sınırlarını bulanıklaştırdığını, buna rağmen hukukî yükümlülüklerin ortadan kalkmadığını vurgular. [29] Gemini entegrasyon boşluğu: Kuruma özgü risk iştahı, tehdit aktörleri, model envanteri, veri tedarikçilerinin güvenilirliği ve kullanıcı davranış ölçümleri burada sayısallaştırılmalıdır.

Öneriler / tasarım gereksinimleri: Chapter, risk bölümünü "etik ek" olarak değil, mimarinin merkez katmanı olarak yazmalıdır. Her operasyonel kullanım durumu için TEVV, provenance, legal review, bias audit, adversarial red-team ve fallback manual mode zorunlu tutulmalıdır. [30]

8. AI dönüşümü Amaç: ML/LLM rolleri, otomasyon, adversarial AI ve güvenlik önlemlerini fonksiyonel düzeyde yerleştirmek.

Metodoloji: NATO'nun 2024 revize AI stratejisi, NIST AI RMF ve AML taksonomisi, NIST GAI profili, MITRE SAFE-AI, IC etik ve AI yönetişim direktifleri, DoD RAI ve AI siber güvenlik kılavuzu. [31] Bulgular: AI'nin en güçlü rolleri bugün itibarıyla observe/orient katmanındadır: sınıflama, anomali tespiti, çok-kaynaklı özetleme, ilişki ağları, örüntü tespiti, segmentasyon ve lojistik öngörü. RAND'ın PLA incelemesi, OODA'nın gözlem ve yönelim adımlarının mevcut AI için daha uygun olduğunu; taktik karar ve icranın ise hâlâ sağlam dünya modelleri ve insan kararına ihtiyaç duyduğunu vurgular. OSINT 2024–2026 stratejisi, GAI'nin tema ve örüntü çıkarma ile özetleme için güçlü olduğunu, ancak hallucination riskleri nedeniyle tradecraft'in güncellenmesi gerektiğini açıkça belirtir. NATO'nun

revize AI stratejisi ise aynı anda AI kullanımını hızlandırmayı, riskleri yönetmeyi ve adversarial AI tehdidine karşı korunmayı hedefler. [32] Gemini entegrasyon boşluğu: Burada kuruma uygun model aileleri ve görev eşlemesi işlenmelidir: hangi görev için küçük uzman model, hangi görev için foundation model, hangi görev için retrieval-augmented kurgu, hangi görev için hiç LLM kullanılmamalı.

Öneriler / tasarım gereksinimleri: Bölüm, AI kullanımını dört role ayırmalıdır: analitik hızlandırıcı, karar seçeneği üreticisi, savunmacı filtre ve kırmızı takım simülatörü. LLM/GenAI için asgari güvenlik paketi; içerik provenance, retrieval-grounding, prompt güvenliği, model izolasyonu, veri minimizasyonu, loglama, düzenli red-teaming, incident disclosure, tedarik zinciri denetimi ve manuel fallback içermelidir. Ayrıca RAI'nin "güveni mümkün kılan hızlandırıcı" olduğu, "yeniliği yavaşlatan fren" olmadığı özellikle vurgulanmalıdır; DoD metinleri bunu açıkça söyler. [33] Gelecek tasarımı ve sözlük

9. 2030 projeksiyonu Amaç: Senaryolar, zaman çizelgesi ve kritik eşikleri tanımlamak.

Metodoloji: NATO Science and Technology Macro Trends 2025–2045, NATO revize AI stratejisi, IC OSINT 2024–2026, RAND'ın 2024/2026 AI ve gelecek savaş çalışmaları ve ODNI veri stratejisi üzerinden 2030'a kadar uzanan analitik projeksiyon yapılmıştır. Bu bölümdeki tarihsel eşikler analitik çıkarım niteliğindedir; doğrulanmış gelecek olayları değildir. [34] Bulgular: 2030'a giderken üç baskın senaryo öne çıkar. Yönetilen adaptasyon senaryosunda, veri kumaşı, provenance, Zero Trust ve RAI kurumsallaşır; AI karar desteği büyür ama insan ajansı korunur. Adversarial hızlanma senaryosunda, deepfake, mikro-hedefleme ve sentetik persona üretimi kamu güvenini eşiğin altına iter; kurumlar doğruluk üretebilse bile yönelim üretemez. Düzeltici normlaşma senaryosunda ise hukukî/etik rejimler, provenance standartları ve eğitim yatırımları rekabeti yavaşlatmaz ama sistemleri daha dayanıklı hâle getirir. NATO'nun makro trend analizi, 2025–2045 bandında "fragmenting public trust" ve AI ile üretilen içeriğin gerçek/sahtesi ayrımını zorlaştırmasını zaten merkez risklerden biri olarak tanımlar. [35] Kritik eşikler: 2030'a kadar özellikle beş eşik izlenmelidir: sentetik içeriklerin insan üretiminden ayırt edilemez hâle gelmesi; kamu

güveni ve kurumsal meşruiyetin kalıcı parçalanması; verinin birlikte işler ve AI-ready hâle gelmesi; insan-makine karar hücrelerinin kalıcı kurumsal forma kavuşması; model/veri/platform tedarik zinciri risklerinin açık çatışma döneminde operasyonel zafiyete dönüşmesi. RAND ve NATO belgeleri, özel sektör bağımlılığı, güven erozyonu ve AI'ye aşırı güvenin bu eşikleri hızlandırabileceğini göstermektedir. [36] Bu zaman çizelgesi, NATO'nun 2025–2045 teknoloji trendleri, ODNI'nin veri/OSINT stratejileri ve RAND'ın AI'nin savaş, propaganda ve insan ajansı üzerindeki etkilerine dair çalışmalarından türetilmiş bir projeksiyondur. [37] Gemini entegrasyon boşluğu: Eğer Gemini verisi belirli ülke veya aktör kümelerine ilişkin saha göstergeleri içeriyorsa, bu zaman çizelgesindeki eşikler bölgesel ve aktör-bazlı olarak ayrıştırılmalıdır.

Öneriler / tasarım gereksinimleri: 2030 projeksiyonu, bölüm sonuna "öngörü" değil "tasarım zorlaması" olarak konmalıdır. Her eşik için ölçülebilir KPI önerilmelidir: sahte içerik tespit süresi, orientation güven puanı, karar zinciri gecikmesi, provenance kapsaması, insan override oranı, red-team başarım oranı.

10. Teknik terimler Bu sözlük, Boyd, JADC2, ODNI veri/OSINT çerçeveleri, NIST AI risk yönetimi, NATO bilişsel harp ve Türkçe kavramsal literatürün birlikte okunmasıyla derlenmiştir. [38]

Sonuç olarak, bölümün omurgası şu önermeyle kapanmalıdır: geleceğin istihbarat başarısı, kimin daha çok veri topladığıyla değil; kimin veri, yönelim, güven, hız, hukuk ve insan ajansını aynı mimaride dengelediğiyle ölçülecektir. Bu, hem RAND/NATO seviyesinde stratejik analitik sistem tasarımının hem de bilişsel güvenlik çağında istihbaratın yeni ontolojisinin çekirdeğidir.

[39] [1] https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html https://www.dni.gov/nctc/jcat/jcat_ctguide/intel_guide.html [2] https://www.act.nato.int/activities/cognitive-warfare/ https://www.act.nato.int/activities/cognitive-warfare/ [3] [7] [8] [13] [38] https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.pdf https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0151_Boyd_Discourse_Winning_Losing.pdf [4] [16]

https://www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf
https://www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf [5] [10] [11] [12]
https://dergipark.org.tr/tr/pub/guvenlikstrtj/article/1646888
https://dergipark.org.tr/tr/pub/guvenlikstrtj/article/1646888 [6]
https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf
https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf [9] [14] [15] [39]
https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF
https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF [17]
https://www.dni.gov/files/documents/ICD/ICD-203.pdf
https://www.dni.gov/files/documents/ICD/ICD-203.pdf [18]
https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.sum.pdf
https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.sum.pdf [19]
https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA595-1/RAND_RRA595-1.pdf
https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA595-1/RAND_RRA595-1.pdf [20]
https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/%24TR-HFM-ET-356-ES.pdf
https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/%24TR-HFM-ET-356-ES.pdf [21] [22]
https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf
https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf [23] https://www.rand.org/pubs/research_reports/RRA853-1.html
https://www.rand.org/pubs/research_reports/RRA853-1.html [24] [25]
https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3161/RAND_RR3161.pdf

https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3161/RAND_RR3161.pdf [26] https://dergipark.org.tr/tr/download/article-file/4365363 https://dergipark.org.tr/tr/download/article-file/4365363 [27] [28] https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf [29] https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf [30] https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF [31] https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy [32] https://www.rand.org/content/dam/rand/pubs/perspectives/PEA4500/PEA4574-1/RAND_PEA4574-1.pdf https://www.rand.org/content/dam/rand/pubs/perspectives/PEA4500/PEA4574-1/RAND_PEA4574-1.pdf [33] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf [34] [35] [36] [37] https://www.nato.int/content/dam/nato/webready/documents/sto/sto_science_and_technology_trends_2025_2045.pdf https://www.nato.int/content/dam/nato/webready/documents/sto/sto_science_and_technology_trends_2025_2045.pdf Katman | Klasik model | Bilişsel harp modeli | Gerekli tasarım ilkesi Toplama | Ayrık INT disiplinleri | Ayrık INT + OSINT + platform telemetrisi + sentetik içerik tespiti | Çok-kaynaklı, sürekli, orkestrasyonlu toplama Veri | Ürün odaklı dosyalar | Veri kumaşı, katalog, API, makine-okur veri, lineage | Görünür, erişilebilir, anlaşılır, bağlı, güvenilir, birlikte işler, güvenli veri Analitik | İnsan-yoğun raporlama | Füzyon, korelasyon, modelleme, segmentasyon, davranışsal telemetri | Analitik + AI + provenance birlikteliği Karar | Komutana sunulan tekil değerlendirme | İnsan-makine karar hücresi, seçenek üretimi, güven

puanları | HMI tasarımı, açıklanabilirlik, güvenilirlik Etki | Bilgi destek faaliyeti | İstihbarat-iletişim-etki entegre kampanyası | OIE/IO ve istihbaratın ortak planlama hücreleri Güvenlik | Ağ çevresi savunması | Zero Trust, model güvenliği, veri hakları, tedarik zinciri | Never trust, always verify; model/veri/platform ayrıştırması Denetim | Sonradan değerlendirme | Sürekli TEVV, incident disclosure, hukuk-etik kapısı | Yaşam döngüsü boyunca ölçme ve düzeltme

Risk sınıfı | Tipik arıza modu | Stratejik etki | Erken gösterge | Asgari kontrol Veri riski | Zehirlenmiş veri, yanlış etiket, köken belirsizliği | Yanlış yönelim ve hatalı hedefleme | Provenance boşlukları, ani model sapması | Veri kökeni, erişim hakları, değişmez kayıt Model riski | Adversarial evasion, prompt injection, model theft | Karar desteğinin manipülasyonu | Beklenmedik çıktı dağılımı, jailbreak izi | Red-team, input/output filtresi, model izolasyonu HMI riski | Aşırı otomasyon güveni, otomasyon yanlılığı | İnsan ajansının aşınması | Operatör override oranının düşmesi | Açıklanabilirlik, güven puanı, insan-onayı Hukukî risk | Sivillerin hedefe dönüşmesi, mahremiyet ihlali | Meşruiyet ve ittifak maliyeti | Yetki belirsizliği, veri minimizasyonu ihlali | IHL/İHK uyum kontrolü, hukuk review

Stratejik risk | Yanlış güven, kriz tırmanması, yanlış caydırma | İstenmeyen eskalasyon | Rakip niyet okumasında aşırı kesinlik | Karşı-varsayım analizi, çoklu senaryo Kurumsal risk | IO-intel rol çatışması, silo, veri kilitlenmesi | Yavaş karar ve zayıf koordinasyon | Eşzamanlı RFI çakışmaları, görev belirsizliği | Ortak görev hücresi, veri standartları Tedarik riski | Kapalı model, opak eğitim seti, dış bağımlılık | Gizli arka kapı ve bağımlılık | SBOM/provenance eksikliği | Tedarik zinciri değerlendirmesi, bağımsız test Toplumsal risk | Güven erozyonu, kutuplaşma, sentetik içerik doygunluğu | Demokratik dayanıklılık kaybı | Güven endeksi düşüşü, viral sahte içerik | İçerik provenance, medya okuryazarlığı, stratejik iletişim Terim | Kısa tanım Bilişsel harp | İnsan zihnini, algıyı, muhakemeyi ve davranışı hedefleyen, çok araçlı etki rekabeti Bilgiye yönelik harp | Bilgi sistemlerine, ağlara, spektruma veya veri altyapısına yönelen teknik saldırılar Orientation | Boyd’a göre gözlem, karar ve eylemi şekillendiren yorumlayıcı merkez ağırlık noktası Decision advantage | Doğru bilgiyi doğru zamanda tanıyıp eyleme çevirebilme ve inisiyatifi koruma yeteneği JADC2 | Tüm alanlarda

sense–make sense–act yaparak bilgi ve karar üstünlüğü üretmeyi amaçlayan yaklaşım Veri kumaşı | Farklı kaynak ve formatlardaki veriyi katalog, erişim ve entegrasyonla ortak düzleme taşıyan katman Provenance | Verinin ve çıktının kökeni, zinciri ve nasıl üretildiğine dair izlenebilirlik TEVV | Test, değerlendirme, doğrulama ve geçerleme çerçevesi RAI | Sorumlu yapay zekâ; etik, güvenlik, yönetişim ve operasyonel güvenin yaşam döngüsü yaklaşımı Adversarial ML | Modeli, veriyi veya çıktıyı manipüle ederek AI sistemini yanıltma alanı Zero Trust | Sürekli doğrulama, en az ayrıcalık ve mikro-segmentasyon esaslı güvenlik mimarisi OIE | Bilgi ortamında harekât; teknik, enformatik ve bilişsel etkilerin birlikte planlandığı operasyon alanı OSINT orkestrasyonu | Açık kaynak toplama gereksinimlerinin, görevlerin ve metriklerin topluluk çapında eşgüdümü Reflexive control | Rakibin kararını, onun algı ve muhakeme çerçevesini etkileyerek dolaylı biçimde yönlendirme mantığı İnsan ajansı | İnsanların sonuç doğuran kurumsal ve toplumsal kararlar üzerindeki belirleyici etkisi

Derinleştirilmiş kavramsal çerçeve

İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp: Zihnin Nihai Savaş Alanı Olarak Yeniden İnşası

1. Kavramsal Çerçeve: Savaşın Doğasındaki Epistemolojik ve Ontolojik Kırılma Yirmibirinci yüzyılın küresel güvenlik mimarisi, savaşın, istihbaratın ve devlet gücünün doğasını kökünden değiştiren derin bir paradigma kaymasına sahne olmaktadır. Tarihsel düzlemde istihbarat faaliyetleri, fiziksel coğrafyalar, düşman kapasiteleri ve stratejik niyetler hakkında veri toplama disiplini olarak tanımlanırken; günümüzde bu tanım, insan zihninin nihai savaş alanı (altıncı harekat alanı) olarak kabul edilmesiyle muazzam bir ontolojik dönüşüm geçirmektedir.1 Geleneksel endüstriyel yıkım ve kitlesel imha modelleri, yerini algı ve anlatı çerçeveleme yarışlarına bırakmıştır.3 Savaş artık yalnızca fiziksel üstünlük kurma veya toprak ele geçirme eylemi değil, doğrudan doğruya düşman unsurlarının (askeri personel, liderler ve sivil toplum) gerçeklik algısını, inanç sistemlerini ve karar alma mekanizmalarını teknolojik ve psikolojik enstrümanlarla yeniden inşa etme mücadelesidir.1 Bu stratejik dönüşüm, yalnızca yeni araçların ve dijital ağların kullanıma girmesinden ibaret değildir; aynı zamanda "gerçeklik" ve "hakikat" kavramlarının tanımlanma biçiminde yaşanan

epistemolojik bir şiddet sürecini temsil eder.2 Bilişsel harp (Cognitive Warfare) disiplini, geleneksel bilgi harekatlarından (Information Operations) veya psikolojik savaştan (PSYOP) kesin çizgilerle ayrılır. RAND Corporation analistleri ve askeri teorisyenler, geleneksel enformasyon harekatlarının sistemleri, veriyi ve taktiksel istihbarat toplamayı hedeflediğini belirtirken; bilişsel harbin, insan beyninin bu veriyi nasıl işleyeceğini, nasıl anlamlandıracağını ve bu anlamlandırma sonucunda nasıl eyleme geçeceğini hedeflediğini vurgulamaktadır.4 Kuzey Atlantik Antlaşması Örgütü (NATO) bünyesindeki Müttefik Dönüşüm Komutanlığı (ACT) İnovasyon Merkezi yöneticisi François du Cluzel ve müttefik stratejistlerin tanımlamalarına göre, bilişsel harp en temelinde bir "bilişsel üstünlük" (cognitive superiority) elde etme kavgasıdır.1 Bu kavga, düşmanın bilişini zayıflatmak, manipüle etmek, geciktirmek veya tamamen yok etmek amacıyla düşmanın karar alma süreçlerine görünmez, ısrarlı ve kümülatif müdahalelerde bulunma sanatı olarak nitelendirilmektedir.1 Modern bilişsel harp, Çinli askeri stratejist Sun Tzu'nun "düşmanı şaşırtma ve gerçek niyetini gizleme" felsefesinin, yapay zekâ ve algoritmalar vasıtasıyla teknolojik olarak ölçeklendirilmiş ve tüm bir nüfusa yansıtılmış halidir.1

Karşılaştırma Boyutu Geleneksel Bilgi Bilişsel Harp ve Bilişsel Harekatları ve Etki Üstünlük Mücadelesi Operasyonları

Bilgi sistemlerinin İnsan bilişi: Algı, yönelme, Öncelikli Hedef Seti bütünlüğü, hedef kitlenin karar ve eylem ikna edilmesi ve spesifik bir mekanizmalarının nörolojik anlatının iletimi.9 ve psikolojik altyapısı.10

Verinin korunması veya Karar alma süreçlerinin Merkezi Amaç bozulması, propaganda rekabet altında bozulması, yoluyla izleyicinin manipüle hedefin yönelim edilmesi.4 yeteneğinin tamamen felç edilmesi.10

Aktörden izleyiciye (actor- Sürekli geri bildirim Etkileşim Modeli to-audience) doğru döngülerine dayalı, dinamik, ilerleyen tek yönlü mesaj uyarlanabilir saldırgan- akışı (Yayın/Propaganda).11 savunmacı etkileşimi.10

Genellikle kısa vadeli, Çok ufuklu: Hem akut Zaman Ufku taktiksel veya belirli bir operasyonel bozulmalar kampanya veya seçim (dakikalar/günler) hem de dönemi ile sınırlı.10 kronik psikolojik şartlandırma (haftalar/yıllar).10

Mesajın ulaşım oranı Karar gecikmesi (latency), Başarı Ölçütü ve Metrikler (erişim), görünürlük, karar hataları, eylem felci, etkileşim (engagement) güvenin erozyonu ve sayıları ve duygu davranış değişikliğinin (sentiment) analizi.10 kalıcılığı.10

Kavramsal mimarinin derinliklerine inildiğinde, devlet ve devlet dışı aktörlerin "ontolojik güvenliklerini" (ontological security) sarsma hedefi göze çarpmaktadır. Ontolojik güvenlik, bir toplumun, devletin veya kurumun tutarlı bir benlik duygusunu ve istikrarlı bir anlatı kimliğini sürdürme ihtiyacı olarak tanımlanır.2 Hibrit çatışma ortamlarında, bir düşmanın ortak benlik duygusunu, tarihsel anlatılarını, ahlaki meşruiyetini veya ulusal amacını bozmak, o devletin fiziksel askeri yeteneklerini yok etmek kadar etkilidir.2 Bu bağlamda "epistemik şiddet", teknolojik altyapıları, biyometrik sensörleri ve algoritmaları kontrol edenlerin bilgi üretimini tekel altına alarak, kitlelerin bilinçaltını soyut algoritmik mantıklar lehine şekillendirmesi sürecidir.2 Merkezi istihbarat yapıları ve savunma aparatları için bu durum, hedef setinin platformlardan ve fiziksel sistemlerden ziyade doğrudan insan bilişine ve toplumsal güven ağlarına doğru genişlemesi anlamına gelmektedir.13

2. Akademik Teoriler ve Geleneksel OODA Döngüsünün Çöküşü Bilişsel harbin askeri karar alma mekanizmaları üzerindeki yıkıcı etkisi ve bu alandaki ontolojik kayma, en net şekilde Albay John Boyd tarafından geliştirilen OODA (Observe-Orient-Decide- Act / Gözlem-Yönelme-Karar-Eylem) döngüsünün teorik çerçevesinin çöküşü ve yeniden inşası üzerinden analiz edilmektedir.14 Tarihsel olarak OODA döngüsü, bir hava muharebe konsepti olarak doğmuş ve düşmandan daha hızlı karar alıp eyleme geçerek, yani döngüyü rakitten daha hızlı tamamlayarak, rakibin bilişsel ve fiziksel uyum sağlama yeteneğini felç etme felsefesine dayanmıştır.15 Ancak modern askeri akademisyenlerin ve Boyd'un kuramını inceleyen stratejistlerin belirttiği üzere, bu teorinin gerçek dehası salt "hız" değil, "Yönelme" (Orientation) aşamasının merkeziliğidir.14 Boyd, Yönelme aşamasını analiz ederken Gödel'in Eksiklik Teoremi, Heisenberg'in Belirsizlik İlkesi ve Termodinamiğin İkinci Yasası (Entropi) gibi derin bilimsel prensiplere atıfta bulunmuştur.14 Bu mantık silsilesi, kapalı bir sistemin (veya dış bilgi akışına kapatılmış manipüle edilmiş bir zihnin) dışarıdan

bağımsız, tutarlı ve eksiksiz bir bilgi üretemeyeceğini, dolayısıyla kendi içine kapanan ve dış dünyadan izole edilen karar alıcıların kaçınılmaz olarak kafa karışıklığı, düzensizlik ve felce (bilişsel entropiye) sürükleneceğini öngörmüştür.14 Bilişsel harp, tam olarak bu kırılganlığı hedef alarak düşmanın Yönelme mekanizmasını zehirler. Eski inançları yıkıp baskı altında yenilerini sentezleyemeyen, yani güncel gerçekliğe yönelim sağlayamayan hedef kuvvet, karar verme aşamasına dahi geçemeden felç olur.14 Güncel akademik literatür, bu bağlamda bilişsel harbi OODA döngüsü etrafında uyarlayarak, Çok Ufuklu Bilişsel OODA Çerçevesi (Multi-Horizon Cognitive OODA Framework) olarak kavramsallaştırmaktadır.7 Bu mimari, operasyonel etkileri Akut (Kısa Ufuklu) ve Kronik (Uzun Ufuklu) olarak iki ana boyutta inceler ve çatışmanın doğasını salt mesajlaşma eyleminden çıkarıp, dinamik bir saldırgan-savunmacı adaptasyon sürecine dönüştürür.

OODA Aşaması Hedeflenen Saldırgan Etki Savunmacı Etki Bilişsel İşlev Kategorisi (Akut Kategorisi (Akut Bilişsel Saldırı) Bilişsel Koruma)

Anında algılama, Hedefin neyi fark Aldatma, yoğun Gözlem (Observe) seçici maruz kalma ettiğini veya gürültü ve manipüle (selective inandırıcı edilmiş bilgi exposure), çevresel bulduğunu seçici ortamında doğru farkındalık maruz bırakma, gözlem kapasitesini kapasitesi ve aldatma veya kasti ve inandırıcılık inandırıcılık bilgi doygunluğu yargılarını tavizsiz yargıları.11 (saturation) ile korumak.11 şekillendirmek.10

Duyusal Çerçeveleme Düşmanca Yönelme (Orient) yorumlama, mekanizmaları, çerçeveleme, anlamlandırma kimlik ipuçları, bilişsel önyargı (sensemaking), duygusal hazırlama istismarı ve yoğun olayları (emotional priming) anlatı baskısına çerçeveleme, veya sahte rağmen sağlıklı nedensel akıl nedensel anlatılar anlamlandırma yürütme ve anlatı yoluyla sürecini baskısı.11 yorumlamayı sürdürmek.11 saptırmak.10

Yargı kalitesi, karar Muhakemeyi bozan Bilişsel stres ve aşırı Karar (Decide) temposu, tereddüt tereddüt, kafa belirsizlik altında yönetimi, bilişsel karışıklığı, manipüle bile karar kalitesini, kısayollara edilmiş aşırı karar temposunu ve (heuristics) olan özgüven veya hatalı özgüveni muhafaza güven, stres altında bilişsel kısayollara etmek.10 özgüven, risk olan güveni algısı.11 artırmak.10

Sahadaki davranış, Erken eylem, yanlış İcra sadakatini Eylem (Act) icra sadakati hizalanmış eylem korumak ve görev (execution fidelity), veya kasti amacını temelden eylemler ve kasti eylemsizlik dâhil zedeleyen, eylemsizlik olmak üzere saldırgan tarafından kararları.11 doğrudan saldırgan tetiklenmiş için faydalı olan eylemleri veya fiziksel veya dijital eylemsizliği proaktif davranışlar ortaya olarak önlemek.10 çıkarmak.10

Akut etkilerin dakikalar veya günler içerisinde ortaya çıkmasına karşın, Çok Ufuklu OODA Çerçevesinin asıl yıkıcı unsuru, haftalar veya yıllar süren Kronik Şartlandırma aşamasıdır.11 Kronik şartlandırma, akut OODA döngüsünün parametrelerini temelden değiştirerek, hedef kitlenin neyi inandırıcı bulduğu, olayları hangi ideolojik çerçeveden okuduğu ve hangi riskleri almaya istekli olduğu gibi temel inançlarını kalıcı olarak yeniden programlar.10 Kurumsal güvenin kademeli olarak aşınması, toplumların kutuplaşması ve yanlış inançların norm haline getirilmesi, bu kronik stratejinin nihai hedefleridir.11 Savunmacının buradaki kronik hedefi ise, otoriter karar alma mekanizmalarına olan güveni ve toplumsal uyumu ne pahasına olursa olsun korumaktır.11

Akademik teoriler bağlamında incelenmesi gereken bir diğer devrimsel konsept, geleneksel bilişsel bilim paradigmalarını yıkan Bedenlenmiş Biliş (Embodied Cognition) teorisidir.6 Geleneksel yaklaşımlar (computationalism), zihni sadece beynin içinde çalışan salt bir bilgi işleme cihazı (bilgisayar) olarak görerek, bedeni ve çevresel etkileşimleri dışlar.6 Oysa bedenlenmiş biliş teorisi, bu Kartezyen dualizmi reddeder. İnsan mantığının, hafızasının, dilinin ve en önemlisi duygularının bedensel, algısal ve motor yeteneklere derinden bağlı olduğunu savunur.6 Bedenlenmiş biliş, üç temel eksende (Kavramsallaştırma, Değiştirme ve Anayasa) şekillenir ve J.J. Gibson'ın Ekolojik Psikoloji kuramlarından, Merleau-Ponty'nin Fenomenolojisine kadar geniş bir entelektüel tabana dayanır.6 Bu teoriye göre, sosyal biliş, zihin okuma teorileriyle değil, ayna nöronlar vasıtasıyla gerçekleşen bedensel ipuçları ve motor taklitleriyle işler.6 Ahlaki biliş ise tamamen fizyolojiktir; kalp atış hızının artması ahlaki yargıları sertleştirirken, iğrenme hissi veya terleme (somatik belirteçler) karar alma sürecini mantıktan önce doğrudan belirler.6 Bilişsel harp stratejistleri bu teoriyi baz alarak, manipülasyonun sadece ekrandaki metinlerle değil, sanal gerçeklik

(VR), somatik işaretleyiciler ve biyometrik geri bildirimler üzerinden insanın doğrudan fizyolojik varlığını hedef alması gerektiğini keşfetmişlerdir.6 NATO Bilim ve Teknoloji Örgütü (STO) ise tüm bu akademik çıkarımları operasyonel bir zemine oturtmak amacıyla Bilişsel Harp Ev Modeli'ni (7 S&T Bilgi Alanı) inşa etmiştir.1 NATO'nun baş bilim insanı raporunda detaylandırılan bu yedi sütun şunları içerir:

1. Durumsal Farkındalık ve Anlamlandırma: Hedeflerin belirsiz durumları anlamlandırmasını sağlayan veya bloke eden faktörlerin incelenmesi.

2. Bilişsel Etkiler: Düşmanın "saptırma, dikkat dağıtma, zayıflatma" gibi doktriner etki fiillerini kullanarak nörobiyolojik bulaşmayı (sosyal bulaşmayı) nasıl tetiklediğinin analizi.

3. Çalışma Yöntemleri (Modus Operandi): Düşmanın psikolojik hazırlama (priming) süreçlerinin ve hilelerinin haritalanması.

4. Teknoloji Sağlayıcıları ve Güç Çarpanları: Yapay zekâ, büyük veri, nörobiyoloji ve biyoteknoloji entegrasyonlarının askeri etkilerinin anlaşılması.

5. Sosyal ve Kültürel Bilimler: Bireysel davranışları şekillendiren yapısal, kültürel ve ekonomik faktörlerin disiplinlerarası incelenmesi.

6. Bilişsel Nörobilim: İnsan beyninin akıl yürütme ve karar verme süreçlerinin altında yatan hücresel ve nörolojik mekanizmaların keşfi.

7. Bilişsel ve Davranışsal Bilimler: İletişim, güven ve duygu mekanizmalarından faydalanılarak savaşçının bilişsel yeteneklerinin korunması ve optimize edilmesi.1

3. Sistem Mimarisi ve Yapay Zekâ Entegrasyonu:

Algoritmik Bilişsel Harp Geleneksel propaganda yöntemleri, "yukarıdan aşağıya" (top-down) tasarlanmış ve geniş kitleleri homojen bir yapı olarak ele alan nispeten kaba ve verimsiz bir mimariye sahipken; modern bilişsel harbin sistem mimarisi, yapay zekâ ile entegre edilmiş "aşağıdan yukarıya"

(bottom-up), hiper-kişiselleştirilmiş ve veri güdümlü bir yapıya bürünmüştür. Özel Rekabetçi Çalışmalar Projesi (SCSP) analistleri ve Çin Halk Kurtuluş Ordusu (PLA) stratejistlerinin literatürü incelendiğinde, bu yeni

nesil sistemin "Algoritmik Bilişsel Harp" (Algorithmic Cognitive Warfare) olarak adlandırıldığı görülmektedir.18 Algoritmik bilişsel harbin sistem mimarisi, hedef kitleleri takip edip davranışlarını analiz eden ileri düzey yapay zekâ istihbarat algoritmaları ile sosyal medya platformlarına yerleştirilmiş, kullanıcının içerik tüketimini görünmez bir şekilde yönlendiren tavsiye (recommendation) algoritmalarının simbiyotik çalışmasına dayanır.18 Çinli askeri akademisyenlere göre, barış ve savaş ayrımını ortadan kaldıran bu mimari, kitlelerin düşüncelerini hedeflenmiş ve esnek bir "bilişsel kozada" (information cocoon) yönlendirebilen yegâne kontrol aracıdır.18 PLA Stratejik Destek Kuvvetleri, Kamu Güvenliği Bakanlığı (MPS) ve Devlet Güvenlik Bakanlığı (MSS) gibi istihbarat kurumlarının eşgüdümüyle yürütülen bu mimari, operasyonel dağılımı mükemmelleştirmiştir.18 Algoritmik Bilişsel Harbin Altı Aşamalı Çerçevesi

Bu sistem mimarisinin işleyiş mekanizması, birbirine sıkı sıkıya bağlı altı entegre aşamadan oluşan bir teorik altyapıya dayanır:

Operasyonel Aşama Algoritmik İşlev ve Taktiksel Hedef

Devasa veri havuzlarından yararlanılarak,

1. Kullanıcı Portresi (User Portrait) bireysel psikolojik profillerin çıkarılması.

Toplumsal düzeyde grupların ideolojik dağılımının ve iç dinamiklerinin dijital bir ikizinin (modelinin) yaratılması.18

Oluşturulan hiper-kişiselleştirilmiş profiller

2. Dikkat Çekme (Attracting Attention) kullanılarak, kullanıcının o anki spesifik duygu durumuna en uygun uyarıcıların seçilmesi ve zihinsel odaklanmanın sağlanması.18

Kurbanın doğal bilişsel eğilimlerini manipüle

3. Referans Önerme (Suggesting edecek olan zehirli veya kutuplaştırıcı Reference) içeriklerin, sanki meşru ve bağımsız bir kaynaktan geliyormuş gibi tavsiye algoritmaları aracılığıyla sunulması.18

Rasyonel filtreleri aşarak öfke, korku,

4. Tepki Uyandırma (Inducing Reaction) sadakat veya panik gibi doğrudan amigdalayı hedef alan somatik ve güçlü duygusal reaksiyonların tetiklenmesi.18

Hedef kitlenin direniş göstermesi veya

5. Zamanında Müdahale (Timely beklenen tepkinin alınamaması durumunda, Intervention) sistemin geri bildirim döngüsü sayesinde otonom olarak yeni bir vektör belirleyip gerçek zamanlı müdahalede bulunması.18

Kullanıcının sürekli olarak kendi yankı

6. Tatmini Denetleme (Supervising odasında (inanç ekosisteminde) tutulması, Gratification) radikalleşme döngüsünün ve bilişsel esaretin kalıcı hale getirilmesi.18

Bu aşamaların sorunsuz çalışabilmesi için, istihbarat mimarisinin devasa ölçekte kişisel "veri hasadı" yapması zorunludur. Algoritmik bilişsel harp, hedef toplumun açık kaynaklı verilerinin yanı sıra, siber hırsızlık (örneğin ABD Personel Yönetimi Ofisi - OPM, Marriott ve Equifax siber saldırıları) yoluyla elde edilen gizli verileri de kullanır.18 Sistem, tekil bir istihbarat "iğnesi" aramak yerine, hedeflerin ticari, sosyal ve psikolojik zaaflarını çapraz korelasyonla (cross-data correlation) eşleştirerek "bütün samanlığı" yutar.18 Geleceğin sistem mimarisinde, yapay zekâ ile desteklenmiş Sanal Gerçeklik (VRE) ve Karma Gerçeklik (XR) cihazlarının üreteceği biyometrik veri havuzları, hedeflerin mahremiyetini tamamen ortadan kaldıracaktır.6 Sistemler, artık kişinin klavye vuruşlarından ziyade, bedensel reaksiyonlarını algoritmik bir silah olarak kullanacaktır.

Biyometrik Veri Kaynağı Ölçüm Odakları ve Algoritmik İstismar ve Psikolojik İfşa Kapasitesi Manipülasyon Potansiyeli

Bilişsel yük, duygusal Bireyin bilinçli olarak dahi Gözbebeği Ölçümü uyarılma, saklı cinsel farkında olmadığı temel (Pupillometry) yönelim, ırksal önyargılar, zaaflara erişim; doğrudan ahlaki yargılar ve şantaj materyali üretimi şizofreni/depresyon veya hiper-kişiselleştirilmiş emareleri.6 korku kampanyalarının tasarımı.6 Hedefin yüzündeki Diplomatik müzakerelerde Yüz Kasları İzleme (EMG - gizlenemez mikro ifadelerin veya askeri sorgularda Elektromiyografi) (Öfke, şaşkınlık, korku, sahte gülümsemelerin,

neşe, iğrenme vb.) tespiti.6 yalanların veya gizli onaylamazlıkların milisaniyeler içinde haritalanması.6

Bilişsel görev zorluğu Sunulan sentetik Elektroensefalografi derecesi, zihinsel propagandanın beyin (EEG) tükenmişlik, dikkat tarafından işlenip dağınıklığı, görsel uyarana işlenmediğinin teyidi; verilen beyinsel odaklanma algoritmik içeriğin hedef düzeyi.6 kitlenin yorgunluk seviyesine göre otonom optimizasyonu.6

Duygusal reaksiyonun Sistemin yarattığı öfke veya Galvanik Deri Tepkisi fizyolojik yoğunluğu, stres korku (somatik belirteçler) (GSR) ve EKG kaynaklı terleme, kalp ritmi düzeyinin hedefe tam ve panik durumu.6 olarak ulaşıp ulaşmadığının kantitatif bir veri olarak doğrulanması.6

IEEE bünyesindeki araştırmalara göre, sentetik medya, sahte personlar (fake personas) ve Bilişsel Ağların (Cognitive Networks) askeri personelle entegrasyonu (APM ve C-APM insan- ajan ekipleri), insan beyninin teknolojiyle tam bir bütünleşme içerisine girmesini sağlamaktadır.22

4. Gerçek Dünya Vakaları ve Operasyonel Yansımalar Bilişsel harbin teorik ve sistemsel kapasiteleri, günümüzde asimetrik ve "gri bölge" (gri bölge) çatışmalarında açıkça uygulanmakta olup, hem devlet destekli makro kampanya düzeyinde hem de taktiksel birey düzeyinde derin operasyonel yansımalar yaratmaktadır.

Tayvan ve Çin Arasındaki Gri Bölge Mücadelesi

Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) raporları ile askeri akademisyenlerin saha araştırmalarına göre, Çin'in Tayvan'a yönelik stratejisi, doğrudan bir kinetik işgalden ziyade, bilişsel harp ve gri bölge operasyonlarıyla Tayvan'ın siyasi, kurumsal ve sivil direncini içeriden çökertmeyi amaçlamaktadır.24 Çin, Birleşik Cephe Çalışmaları (United Front Work) aracılığıyla Tayvan'daki medya organlarını, iş dünyasını, dini kurumları ve siyasi elitleri ko-opte etme (işbirliğine zorlama) girişimlerinde bulunmaktadır.25 Çin, Tayvan yönetimine karşı sürekli bir "silahlı yeniden birleşme" (armed reunification) ve "savaşa çekilme" davulu çalarak, kitleler üzerinde yoğun bir psikolojik basınç ve bilişsel baskı oluşturmaktadır.27 "Spamouflage" adı verilen devlet destekli operasyonlarda, yapay zekâ ile güçlendirilmiş Büyük Dil Modelleri, Tayvanlı yetkililerin veya Batılı

muhaliflerin dijital ayak izlerini takip ederek eşzamanlı duygu analizi (sentiment analysis) yapmakta ve hedeflenmiş taciz kampanyaları düzenlemektedir.18 CSIS analizleri, bu stratejilerin ABD'li politika yapıcılar üzerinde bir "gölge risk" (shadow risk) yarattığını; kriz tırmanışından kaçınma arzusunun, gelecekteki uyuşmazlıklarda daha tehlikeli ve çözümsüz çatışmalara zemin hazırladığını vurgulamaktadır.26 Amaç, Tayvan'ın savunulmaya değer olmadığına dair bölgesel inancı kırmak ve işgale fiziki/psikolojik bir zemin hazırlamaktır.21 Rusya'nın Ontolojik Saldırıları ve Batı Demokrasileri

Rusya'nın NATO müttefiklerine ve Baltık ülkelerine yönelik stratejisinde, konvansiyonel askeri yığınak veya siber harekatlar yalnızca destekleyici bir role sahipken; asıl stratejik belirleyici güç bilişsel ve enformasyonel araçlardır.29 Moskova'nın, askeri doktrininde "Refleksif Kontrol"

(Reflexive Control) olarak kavramsallaştırdığı strateji, hedef alınan liberal demokrasilerin içindeki etnik, sosyal ve siyasi fay hatlarını yapay zekâ destekli bot ve troll ağlarıyla kışkırtmaya dayanır.19 Amaç, hedef kitlelerin "ne düşündüğünü değiştirmek" ve bunun üzerinden "nasıl davrandıklarını" veya "nasıl oy verdiklerini" manipüle etmektir.21 Rusya'nın devlet destekli medya organları (RT ve Sputnik gibi) üzerinden yürüttüğü bilgi enjeksiyonları, alternatif epistemolojiler ve komplo teorileri yaratarak gerçeğin kendisini bulanıklaştırır.2 Sidney bıçaklama senaryosunda (Sydney stabbing scenario) da görüldüğü üzere, sahte personlar ve sentetik medya aracılığıyla üretilen yapay gerçeklikler, savaşçıların ve politika yapıcıların karar alma süreçlerini temelden felç etmekte, sahte olanla gerçeğin ayırt edilemez hale gelmesine neden olmaktadır.23

Otonom Bilişsel Suikast: "Uzman Çavuş Jones" Senaryosu

Bilişsel harbin birey seviyesindeki hiper-kişiselleştirilmiş potansiyelini anlamak için, yapay zekâ destekli tehditleri inceleyen "Uzman Çavuş Jones" senaryosu, modern savaşın ulaştığı tehlikeli sınırı göstermektedir.21 Bu projeksiyonda, düşman bir yapay zekâ istihbarat sistemi, ABD askeri olan Jones'un sosyal medya geçmişini inceleyerek onun fevri, nevrotik ve şiddete eğilimli bir psikolojik yapıya sahip olduğunu sadece 20 saniye içinde tespit eder.21 Algoritma, Jones'un eşi Carla ve birliği içindeki Çavuş Martinez'in sosyal medyadaki açık kaynaklı fotoğraflarını harmanlayarak, bu iki ismin

çıplak hallerini yüksek doğrulukla simüle eden ve cinsel ilişkiye girdiklerini gösteren sentetik bir "deepfake" video üretir.21 Bu video, isimsiz bir hesap üzerinden Jones'a gönderilir. OODA döngüsü tamamen bozulan, gerçeklik algısı felç olan ve şiddet eğilimi tetiklenen Jones, rasyonel düşünme yetisini kaybederek evine döner, eşini bir çekiçle öldürür ve ardından intihar eder.21 Bu vaka, tek bir mermi dahi harcanmadan, sıfır lojistik maliyetle, son derece eğitimli bir askeri unsurun kendi zihinsel zaafları kullanılarak dakikalar içinde otonom bir yapay zekâ tarafından nasıl elimine edilebileceğini kanıtlayan en dehşet verici operasyonel yansımadır.21

5. Mekanizma Analizi: Nöro-Psikolojik İstismar ve Karar Alma Dinamikleri Bilişsel harbin eşi görülmemiş başarısı, insan zihninin her zaman rasyonel kararlar alan kusursuz bir bilgi işlem cihazı olduğu yönündeki asırlık varsayımları reddetmesine ve hedefin biyolojik, duygusal ve psikolojik köklerine (amigdala, evrimsel önyargılar, somatik belirteçler) cerrahi bir hassasiyetle inmesine dayanır.6 Araştırmacı Rand Waltzman ve diğer istihbarat analistlerinin vurguladığı üzere, duygular rasyonel düşünceye bir engel veya sapma değil; aksine, savaş koşullarında bile rasyonel karar almanın temel yapıtaşıdır.6 Askeri liderlerin ve sivil kitlelerin karar alma mekanizmalarını şekillendiren temel vektör "duygusal risk algısıdır". Duyguların savaş stratejisi üzerindeki mekanizması şu şekilde işler 6:

● Korku ve Üzüntü (Riskten Kaçınan Duygular): Karar alıcılara korku enjekte edildiğinde, durum denetiminden çıktıklarını hissederler. Amigdalanın tetiklenmesiyle stratejistler daha kötümser olur ve siber saldırı veya kısıtlı hava gücü gibi riski daha düşük, güvenli ancak stratejik etkisi sınırlı askeri güç formlarına yönelirler.6 1870-1871 Fransa-Prusya Savaşı'nda Şansölye Otto von Bismarck, dış güçlerin müdahale etmesinden duyduğu yoğun korku (fear) nedeniyle Paris'in derhal bombalanmasını emrederek riski minimize etmeye çalışmıştır.6

● Öfke (Risk Alan Duygular): Öfke enjekte edildiğinde ise stratejistler durumun tamamen kontrolleri altında olduğu yanılgısına düşerler. Bu sahte özgüven, onları düşmanı yok etmek için kara harekatı (landpower) gibi aşırı riskli, yüksek maliyetli ve öngörülemez eylemlere sürükler.6 Prusya halkının aynı savaşta Paris'in bombalanmasını istemesi tamamen öfke ve tarihsel nefret (hatred) kaynaklıdır.6

Sistem, insan beyninin varsayılan düşünme yöntemlerini, hızlı karar almak için evrimleştiği sezgisel (heuristics) kestirmeleri ve bilişsel önyargıları birer biyolojik güvenlik açığı olarak kullanır.21 Duygusal beklentiler, isyancı grupların veya devletlerin şiddet kullanma kararlarını dahi belirlemektedir; bazı terör örgütleri, karşı toplumda aşırı bir nefret (ve dolayısıyla acımasız bir mukabele) yaratmamak adına kasti olarak eylemsizliği seçebilmektedir.6 Sanal Ortamlarda Mimikri ve Yüz Birleştirme (Face-Morphing) Dinamikleri

Bilişsel manipülasyonun derin mekanizmalarından bir diğeri, Sanal Gerçeklik Ortamlarında (VRE) gerçekleştirilen "mimikri" (taklit) tekniğidir.6 Stanford Üniversitesi'nden araştırmacıların (Bailenson, Iyengar ve Yee) yürüttüğü devrim niteliğindeki deneyler, dijital yüz birleştirme teknolojisinin oy verme davranışları üzerindeki korkunç etkisini ortaya koymuştur.6

● Yapılan deneylerde, gerçek veya sentetik bir politikacının dijital görüntüsünün içine, o an ekran başında olan hedefin (seçmenin) yüz hatlarının %40'ı oranında gizlice entegre edilmiştir.

● Seçmenlerin güçlü bir partizan kimliğe sahip olmadığı senaryolarda, bu gizli manipülasyonun kararsız seçmenlerin %20'sinin oyunu, yüzü kendisine benzeyen adaya kaydırdığı görülmüştür.6

● Bu mekanizma, evrimsel biyolojideki "akrabalık seçimi" (kin selection) ve sosyal psikolojideki "aşinalık/maruz kalma etkisi" (mere exposure) ile çalışır. İnsan beyni, kendisine fiziksel olarak benzeyen (genetik bağ algısı yaratan) yüzleri bilinçaltında daha güvenilir, cazip ve ikna edici bulacak şekilde programlanmıştır.6 Seçmenler, ekrandaki adayın yüzünün aslında kendi yüzlerinin bir kopyası olduğunu asla fark edememiştir.6 Bu klinik veriler, VRE'lerin askeri ve sivil alanlarda hedeflerin spesifik fobilerini (yükseklik/acrophobia, uçuş/aviophobia, örümcek/arachnophobia) tetikleyerek ağır anksiyete ve boyun eğme yaratmak için kullanılabilecek mükemmel bir "epistemik silah" mekanizması sunduğunu göstermektedir.6 Buna ek olarak, "Yapay Zekâ Bal Küpleri" (AI Honey Pots) üzerinden geliştirilen parasosyal ilişkiler mekanizması da, devlet yetkililerinin duygusal zaaflarını hedef alır. Sentetik profiller, yalnızlık çeken veya duygusal boşlukta olan askeri personelle romantik bağlar kurarak, onların gizli şifrelerini, kurumsal sırlarını ve kişisel korkularını hasat eder.21 Bu

parasosyal zihinsel esaret, personeli sabotaja, ihanete veya 2021'de Belçika'da yaşandığı gibi doğrudan intihara sürükleyecek kadar etkilidir.21

6. Trend Analizi (2020–2026): Yükselen Tehdit Vektörleri 2020 ile 2026 yılları arasındaki stratejik konjonktür, büyük güç rekabeti ve yapay zekâ alanındaki eksponansiyel teknolojik sıçramalar, bilişsel harbin araçsal yeteneklerinde logaritmik bir artışa neden olmuştur. Gelecek çatışma ortamlarında "Bilişsel Üstünlüğü" sağlamayı giderek zorlaştıracak temel eğilimler (trendler) şunlardır:

1. Üretken Yapay Zekâ (GenAI) ve Otonom Bilişsel Operasyonlar

Geçmişte devlet destekli hacker grupları ve insan troller üzerinden manuel olarak yürütülen dezenformasyon kampanyaları, 2023 sonrası süreçte ChatGPT gibi Büyük Dil Modellerinin (LLM) devreye girmesiyle devasa bir endüstriyel otomasyona geçmiştir.18 Otonom ajanlar, hedeflerin duygu analizini gerçek zamanlı yaparak, saniyeler içinde binlerce farklı dilde, kültürel nüanslara hakim sentetik içerik (makale, deepfake video, ses kaydı) üretebilmektedir. Yapay zekâ, insanların verdiği tepkileri gerçek zamanlı analiz ederek, hedefe en uygun taktiksel söylemi bir "A/B testi" hızıyla optimize etmekte ve savunma sistemlerinin reaksiyon süresini (OODA döngüsünü) sıfıra indirmektedir.21

2. Askeri Metaverse ve Yeni Saldırı Yüzeyi

Savunma sanayi trendleri, eğitim ve komuta kontrol mimarisinin "Askeri Metaverse" (Military Metaverse) ortamlarına taşınmasına işaret etmektedir. Savaşın bu yeni sanal katmanı (Synthetic Environments), askeri personelin karmaşık savaş alanlarını simüle etmesi, PME (Profesyonel Askeri Eğitim) reformu, gelişmiş işe alım süreçleri (NFT teşvikleri, eSpor entegrasyonu), döngüsel silah testi ve personelin sosyal/aile desteği alması gibi muazzam taktik avantajlar sunmaktadır.6

Askeri Metaverse'in Sunduğu Taktik ve Bilişsel Harp Açısından Gelişim Alanları Operasyonel Avantajlar Yarattığı Güvenlik Açıkları

Personelin savaşın "sisini ve Düşman sızmaları halinde Sürükleyici Sentetik sürtünmesini" son derece sentetik ortama korku veya Eğitim gerçekçi karma gerçeklik panik yaratacak sahte ortamlarında, risk almadan

senaryoların (dost ateşi vb.) deneyimlemesi.6 manipüle edilerek yerleştirilmesi ihtimali.6

Personelin oyun ve eğitim Personelin davranışsal ve Bütünsel Personel içindeki gizli liderlik biyometrik verilerinin Değerlendirmesi yeteneklerinin, risk (hedefleme paketleri - toleransının ve becerilerinin targeting packages) yapay zekâ ile sürekli düşman istihbaratı ölçülmesi.6 tarafından ele geçirilmesi ve profillenmesi.21

Askeri üslerdeki refah Düşman ajanlarının veya Sosyal ve Ailevi Destek programlarının, sağlık yapay zekâ "bal küplerinin", Ağları hizmetlerinin ve askeri personelin yalnızlığını çocukların eğitiminin sanal sömürerek ailevi moral ortama entegrasyonu.6 çöküşü yaratması ve parasosyal sızmalar yapması.21

Ancak bu entegrasyon, kullanıcıların "mevcudiyet" (presence) ve "bedenlenme" (embodiment) hislerini kullandığı için, düşman algoritmaların askeri personelin beyin fonksiyonlarına doğrudan biyometrik sızma yapabileceği devasa bir saldırı yüzeyi yaratmaktadır.6

3. Transhümanizm, Nöroteknoloji ve Doğrudan Fizyolojik Saldırılar

2026 ufku itibarıyla, bilişsel müdahaleler sadece psikolojik (propaganda) değil, fizyolojik ve nörolojik boyutlara taşınmıştır.13 Çin Halk Kurtuluş Ordusu'nun (PLA) vizyonu, insan ile bilgi teknolojisi sistemlerinin birleştirildiği bir "transhümanist sistemler sistemi" (transhuman system of systems) yaratmaktır.21 Bununla birlikte, yönlendirilmiş enerji, sonik veya mikrodalga silahlarının (Himalayalar'daki çatışmalarda kullanıldığı rapor edilen silahlar gibi) donanım olarak doğrudan insan beynini hedef alması, personelin nöral ağlarına kalıcı fiziksel hasar verilmesine ve karar alma yetisinin tamamen yok edilmesine imkân tanımaktadır.17 Beyin, bir biyolojik veri işleme aygıtı olarak doğrudan hedef tahtasındadır.13

7. Stratejik Sonuçlar ve Savunma Tavsiyeleri Geleneksel kinetik çatışma konseptlerinden ve Soğuk Savaş bilgi harekatı doktrinlerinden farklı olarak, bilişsel harbin asimetrik, sürekli ve görünmez doğası, devletlerin ve ulus-üstü ittifakların (NATO) güvenlik stratejilerini temelden değiştirmesini zorunlu kılmaktadır.1

Stratejik ve Ontolojik Sonuçlar:

1. Düşmanlık ve Barış Arasındaki Çizginin Silinmesi: Savaş artık coğrafi ve fiziki bir alana sıkışmamıştır. Barış zamanında dahi kesintisiz olarak yürütülen, silahlı çatışma eşiğinin altında kalan gri bölge (gri bölge) operasyonları, toplumları ve askeri unsurları sonsuz bir bilişsel harpın içinde tutmaktadır.1 Hedef seti artık tanklardan, gemilerden ve tesislerden ziyade; kurumsal meşruiyet, ortak kimlik anlatıları ve ulusal güven ağlarıdır.13

2. Epistemik Şiddet ve Gerçeğin Yitimi: Bilişsel harbin en büyük kurbanı, demokratik toplumlarda mutabakat sağlanan gerçekliğin kendisidir.2 Toplumlar, yapay zekâ tavsiye algoritmaları eliyle birbirine düşman "bilişsel kozalara" hapsedildiğinde, asgari bir sivil tartışma yürütmek için gereken ortak epistemolojik zemin kaybolmaktadır.2 Teknoloji şirketleri ve platform yöneticileri, bu yeni savaşın istem dışı veya mecburi aktörleri haline gelmiştir.2

3. Başarının Yeniden Tanımlanması (Karar Merkezli Değerlendirme): Bilişsel çatışmalarda başarı artık ne kadar verinin manipüle edildiğiyle veya görünürlükle değil, düşmanın karar kalitesinin ne kadar düşürüldüğüyle (Decision Degradation) ölçülmektedir.10 Eğer hedef kuvvet eylemsiz kalıyorsa, gereksiz hedeflere saldırıyorsa veya kendi müttefiklerine şüpheyle yaklaşıyorsa, bilişsel harp saldırgan açısından kesin bir zafere ulaşmış demektir.7 Bilişsel Savunma ve Stratejik Direnç İçin Operasyonel Tavsiyeler: Bu varoluşsal ve sistemik tehdide karşı koymak adına savunma mimarisinin, "Çok Ufuklu Bilişsel OODA Çerçevesini" merkeze alacak şekilde acilen revize edilmesi şarttır 11:

● Bilişsel Bağışıklık Sistemi (Cognitive Inoculation) İnşası: Askeri personel ve sivil karar alıcılar, sanal ortam manipülasyonlarına, deepfake teknolojilerine ve duygusal hedeflemelere karşı sürekli bir farkındalık eğitimine tabi tutulmalıdır.6 Psikoloji ve nörobilim literatüründen faydalanılarak, tıpkı biyolojik virüslere karşı yapılan aşılamalar gibi, zihinler sentetik tehdit simülasyonlarıyla proaktif olarak aşılanmalıdır (inoculation).6 Duygusal manipülasyon tekniklerinin kapsamlı bir taksonomisi oluşturulmalı ve komuta kademelerine entegre edilmelidir.6

● NATO STO Ev Modeline Dayalı Savunma İkilemi: Savunma stratejisi üç temel fonksiyona dayanmalıdır: Düşmanın etki operasyonlarını yürütme kapasitesini degrade etmek (Degrade Adversary Capabilities), mevcut insan ve teknoloji birleşiminin bilişsel kapasitesini temel seviyenin üzerine çıkarmak (Improve Cognition) ve siber-bilişsel stres altında görev operasyonlarını sürdürebilecek sağlam bir direnç inşa etmek (Build Resilience).1 Karar Koruma (Decision Protection) ve Eylem Koruma (Action Protection) doktrinleri, ulusal güvenlik strateji belgelerine ana unsurlar olarak eklenmelidir.10

● Otomatize Edilmiş Kontrol Ajanları (C-APM): Düşman yapay zekâsının hız ve veri işleme avantajı göz önüne alındığında, savunmanın sadece insan analistlerin muhakemesine bırakılması taktiksel bir intihardır. Bilişsel saldırıları (yüz morphing, biyometrik veri hırsızlığı, parasosyal sızmalar) milisaniyeler içinde tespit edecek, engelleyecek ve gerektiğinde karşı taarruza geçecek kendi otonom yapay zekâ savunma ajanlarımızın sisteme dahil edilmesi elzemdir.6 Neticede, algıların, duyguların ve nörolojik süreçlerin hedeflendiği bu yeni ontolojik mücadelede nihai zafer, salt en çok veriye veya en gelişmiş geleneksel silaha sahip olanın değil; dışsal gürültüye, aşırı stres koşullarına ve algoritmik manipülasyonlara rağmen OODA döngüsünü sağlam tutabilen, gerçeği sentetik olandan ayırabilen ve kendi kararlarının otonom mimarı kalabilen (adaptability) sistemlerin olacaktır.1 Stratejik istihbarat biliminin ve operasyonel sanatın yeni kutsal kâsesi, artık sadece düşman bilgisinin toplanması değil, bizzat müttefik insan zihninin egemenliğinin ve ontolojik bütünlüğünün korunmasıdır.

Alıntılanan çalışmalar

1. Cognitive warfare: NATO chief scientist research report, erişim tarihi Haziran 2, 2026, https://www.sto.nato.int/wp-content/uploads/chief-scientist-report- cognitive-warfare-final.pdf

2. War Without Borders: - TRT World Research Centre, erişim tarihi Haziran 2, 2026, https://researchcentre.trtworld.com/wp-content/uploads/2025/08/War-Without- Borders.pdf

3. Winning Influence in the Cognitive Domain | Small Wars Journal by Arizona State University, erişim tarihi Haziran 2, 2026, https://smallwarsjournal.com/2026/03/06/winning-influence-in-the-cognitive-domain/

4. Information Operations - RAND, erişim tarihi Haziran 2, 2026, https://www.rand.org/topics/information-operations.html

5. Psychological Warfare - RAND Corporation, erişim tarihi Haziran 2, 2026, https://www.rand.org/topics/psychological-warfare.html

6. Future Challenges to Cognitive Superiority – Irregular Warfare Center, erişim tarihi Haziran 2, 2026, https://irregularwarfarecenter.org/publications/perspectives/future-challenges- to-cognitive-superiority/

7. Cognitive Warfare: Definition, Framework, and Case Study - arXiv, erişim tarihi Haziran 2, 2026, https://arxiv.org/pdf/2603.05222

8. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone - National Defense University, erişim tarihi Haziran 2, 2026, https://www.ndu.edu/News/Article-View/Article/3856627/cognitive-warfare-the- fight-for-gray-matter-in-the-digital-gri bölge/

9. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive..., erişim tarihi Haziran 2, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/

10. Cognitive Warfare: Definition, Framework, and Case Study - arXiv, erişim tarihi Haziran 2, 2026, https://arxiv.org/html/2603.05222v1

11. Defining Cognitive Warfare: A NDAA Mandate Response, erişim tarihi Haziran 2, 2026, https://smallwarsjournal.com/2026/05/05/defining-cognitive-warfare/

12. Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs - CSIS, erişim tarihi Haziran 2, 2026, https://www.csis.org/analysis/beyond- bullets-and-bombs-rising-tide-information-war-international-affairs

13. Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness > Institute for National Strategic Studies > View Publications, erişim tarihi Haziran 2, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4371195/cognitive-warfare-2026-natos- chief-scientist-report-as-sentinel-call-for-operat/

14. The Dialectic of Deception: John Boyd and the Cognitive Battlefield, erişim tarihi Haziran 2, 2026, https://warontherocks.com/the-dialectic-of-deception-john- boyd-and-the-cognitive-battlefield/

15. Cognitive Warfare and Organizational Design: Leveraging AI to Reshape Military Decisionmak - NDU Press, erişim tarihi Haziran 2, 2026, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/4368980/cognitive-warfare-and-organizational-design-leveraging- ai-to-reshape-military-d/

16. Cognitive Warfare | The Cove - Australian Army, erişim tarihi Haziran 2, 2026, https://cove.army.gov.au/article/cognitive-warfare

17. Cognitive warfare: the new battlefield exploiting our brains - Polytechnique Insights, erişim tarihi Haziran 2, 2026, https://www.polytechnique- insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield- exploiting-our-brains/

18. Decoding-Chinas-AI-Powered-'Algorithmic-Cognitive-Warfare-Final.pdf - SCSP, erişim tarihi Haziran 2, 2026, https://www.scsp.ai/wp-content/uploads/2024/11/Decoding-Chinas-AI- Powered-%E2%80%98Algorithmic-Cognitive-Warfare-Final.pdf

19. 212 Libby Lange on Algorithmic Cognitive Warfare - Information Professionals Association, erişim tarihi Haziran 2, 2026, https://information-professionals.org/episode/cognitive-crucible-episode-212/

20. Our Work - SCSP, erişim tarihi Haziran 2, 2026, https://www.scsp.ai/ourwork/

21. The Challenge of AI-Enhanced Cognitive Warfare: A Call to Arms for..., erişim tarihi Haziran 2, 2026, https://smallwarsjournal.com/2025/01/22/the-challenge-of- ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/

22. Cognitive Warfare- Statuse, Challenges and Future Trendse - IEEE Xplore, erişim tarihi Haziran 2, 2026, https://ieeexplore.ieee.org/iel8/11063697/11063744/11064284.pdf

23. Designing AI-Enabled Countermeasures to Cognitive Warfare - NATO, erişim tarihi Haziran 2, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/S TO-MP-HFM-377/MP-HFM-377-06.pdf

24. Viewing China's Cognitive Warfare Through the Lens of Its Global Strategy - National Intelligence University, erişim tarihi Haziran 2, 2026, https://www.ni-u.edu/wp-content/uploads/2026/03/NIUShort_20260318_DNI_2025_04082.pdf

25. China's Way of Occupation: Implications for Taiwan - Irregular Warfare Center, erişim tarihi Haziran 2, 2026, https://irregularwarfarecenter.org/publications/research-studies/chinas-way-of- occupation-implications-for-taiwan/

26. Shadow Risk: What Crisis Simulations Reveal about the Dangers of Deferring U.S.

Responses to China's Gray Zone Campaign against Taiwan - CSIS, erişim tarihi Haziran 2, 2026, https://www.csis.org/analysis/shadow-risk-what-crisis- simulations-reveal-about-dangers-deferring-us-responses-chinas

27. The Taiwan Strait Game Between China and the United States: Risk Variables and Crisis Management - Interpret, erişim tarihi Haziran 2, 2026, https://interpret.csis.org/translations/the-taiwan-strait-game-between-china-and-the-united-states-risk-variables-and-crisis-management/

28. CSIS' war games, designed for cognitive warfare against China, will have little influence - Global Times, erişim tarihi Haziran 2, 2026, https://www.globaltimes.cn/page/202208/1273757.shtml

29. Cognitive Warfare - Belfer Center, erişim tarihi Haziran 2, 2026, https://www.belfercenter.org/sites/default/files/pantheon_files/2019-11/CognitiveWarfare.pdf

30. How to Lose an Information War in 10 Days - CSIS, erişim tarihi Haziran 2, 2026, https://www.csis.org/analysis/how-lose-information-war-10-days

31. Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict - PMC, erişim tarihi Haziran 2, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12460417/

32. [2504.11486] Designing AI-Enabled Countermeasures to Cognitive Warfare - arXiv, erişim tarihi Haziran 2, 2026, https://arxiv.org/abs/2504.11486

Bölüm Değerlendirme ve Derinleştirme Dosyası

Bu bölümün geniş okuması yapılırken bilişsel harp ve ontolojik dönüşüm yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiği dir. Bu nedenle bölümün analitik omurgası karar vericinin yönelim katmanı, güven mimarisi, sentetik içerik ve veri kökeni üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir. Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar. Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle bilişsel harp ve ontolojik dönüşüm alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?
  - Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi?
  - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?
  - YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı?
  - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?
  - Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı?
  - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

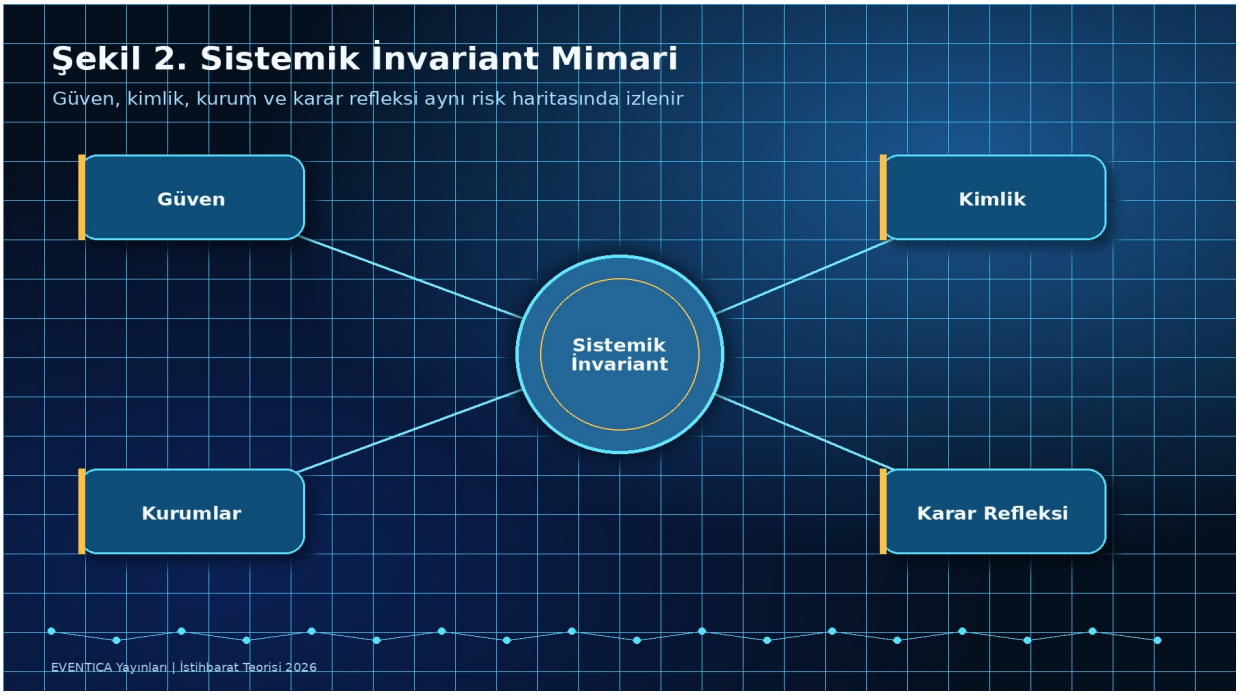
Araştırma Soruları

1. İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp alanında en güçlü erken uyarı göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?
3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?
4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma sağlanmalıdır?
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı anlamlara gelir?
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?
8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 2. Sistemik İnvariantlar ve Sosyal Sistemlerin Hedef Alınması

Bir toplumun asıl savunması sadece güvenlik duvarı veya askeri kapasite değildir; epistemik yapı, sosyal güven, ortak kimlik ve gelecek tahayyülüdür.



Şekil 3. Sosyal sistemlerin korunması gereken invariant yapıları

Tablo 5. Sistemik invariant sınıflandırması

Invariant	İstihbarattaki anlamı	Kırılma riski
Epistemik yapılar	Neyin doğru kabul edildiğini belirleyen kurum ve pratikler	Hakikat kriterlerinin dağılması
Aksiyolojik hiyerarşi	Toplumun değer öncelikleri	Etik pusulanın manipülasyonu
Kimliksel yapılar	Biz/öteki ayrımı ve tarihsel hafıza	Kutuplaşma ve aidiyet kırılması
Sosyal güven mimarisi	Yatay ve dikey güven ilişkileri	Kurumlara güven kaybı
Teleolojik projeksiyon	Ortak gelecek fikri	Stratejik irade kaybı

Bölüm 2: Sistemik İnvariantlar ve Çoğullamalı Mimariler: Sosyal Sistemlerin Epistemik Çerçevelerinin, Güven Yapılarının ve Kolektif Kimliklerinin Hedef Alınması

Kavramsal Çerçeve Modern güvenlik ve stratejik istihbarat paradigması, geleneksel siber savaş ve enformasyon operasyonlarının yapısal sınırlarını aşarak doğrudan sosyal sistemlerin ontolojik temellerini hedef alan yeni bir çatışma evresine geçiş yapmıştır. Bu evre, akademik literatürde ve askeri doktrinlerde "bilişsel harp" (cognitive warfare) olarak adlandırılmaktadır. NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından 2026 yılında yayımlanan güncel stratejik araştırmalar, bilişsel harbi basitçe bir dezenformasyon faaliyeti veya teknolojik manipülasyon olarak değil, hedef toplumun ne bildiğini değil; bilgiyi nasıl anlamlandırdığını, nasıl güven inşa ettiğini, gerçekliği nasıl algıladığını ve entegre bir bütün olarak nasıl koordine olduğunu belirleyen temel ontolojik yapı taşlarına yönelik yapısal bir saldırı olarak yeniden kavramsallaştırmaktadır.1 Geleneksel propaganda yöntemleri, belirli bir fikrin benimsetilmesini veya reddedilmesini amaçlarken; bilişsel harp, bir sosyal sistemin kendi kendini yönetme, gerçeği analiz etme ve uyum sağlama kapasitesini temelden felce uğratmayı stratejik bir hedef olarak belirler.4 Bu yeni kavramsal çerçevenin merkezinde "sistemik invariantlar" (systemic invariants) teorisi yer almaktadır. Karmaşık sosyo-teknik sistemlerin güvenlik analizlerinden bilişsel harp doktrinine uyarlanan sistemik invariant kavramı, bir sistemin dış çevresindeki yapısal ve işlevsel dönüşümlere, yüksek etkili stokastik şoklara ve enformasyonel çalkantılara rağmen temel kimliğini, süreçlerinin yeniden üretimini ve tutarlılığını korumasını sağlayan değişmez ontolojik özellikleri ifade eder.4 Bu invariantlar, bir toplumun veya kurumun bilişsel mimarisinin "ontolojik iskelesini" oluşturur. Sistemin alt bileşenleri arasındaki bağlantısallığı güvence altına alır, adaptif dönüşümlerin sınır koşullarını belirler ve yüksek belirsizlik altında bile stratejik kendi kaderini tayin etme yetisini ayakta tutar.4 Sistemik invariantlar stratejik analiz bağlamında beş ana kategoride sınıflandırılır:

1. Epistemik Yapılar: Bir toplumun veya sistemin neyi doğru kabul ettiğini belirleyen ortak hakikat kriterleri, bilgi doğrulama süreçleri ve gerçeği değerlendirme standartlarıdır.

Epistemik invariantlar, bağımsız bilim kurulları, yargı organları ve güvenilir medya ekosistemleri gibi kurumsal yapılar aracılığıyla ayakta tutulur.4

2. Aksiyolojik Hiyerarşiler: Toplumun kolektif tercihlerini, etik kodlarını ve ahlaki pusulasını yönlendiren değerler bütünü ve bu değerlerin birbirine olan öncelik sıralamasıdır.3

3. Kimliksel (Identificatory) Yapılar: Sistemin tarihsel hafızası, grubun aidiyet kavramları, "biz" ile "öteki" arasındaki sınırların nasıl çizildiği ve kolektif benlik algısının hangi öyküler üzerine inşa edildiğini belirleyen yapısal unsurlardır.4

4. Sosyal Güven Mimarileri: Devlet kurumlarının siyasi ve bürokratik meşruiyeti, vatandaşların birbirlerine duyduğu yatay güven, otoriteye duyulan dikey güven ve toplumsal bağların şoklara karşı dayanıklılık eşiğidir.4

5. Teleolojik Projeksiyonlar: Sosyo-teknik sistemin ortak bir geleceğe yönelik olarak paylaştığı vizyon, umut ve stratejik hedef birliğidir. Toplumun kendi geleceğini inşa etme iradesini temsil eder.4 Bilişsel harp stratejileri, bu sistemik invariantları hedef alarak sistemin "bilişsel dekoherans"

(cognitive decoherence) adı verilen bir parçalanma ve anlamsızlaşma evresine sürüklenmesini amaçlar. Bilişsel dekoherans, yapısal olarak koşullandırılmış ve potansiyel olarak geri döndürülemez bir bilişsel egemenlik erozyonudur.7 Bu duruma düşen bir sosyo-teknik sistem, fiziksel veya kurumsal olarak çökmese dahi, entegre bir bilişsel düzen olarak gerçekliği tutarlı bir şekilde algılama, kendini geliştirme, adaptasyon sağlama ve dış tehditlere karşı organize bir biçimde kendini savunma kapasitesini bütünüyle kaybeder.4 Bu aşındırma sürecinin stratejik ve ontolojik açıdan en tehlikeli özelliği "kurucu görünmezlik"

(constitutive invisibility) prensibi etrafında şekillenmesidir.4 Bir sisteme yönelik kinetik veya yıkıcı siber saldırılar (örneğin kritik altyapıların çökertilmesi) sistem tarafından dışsal bir saldırı olarak hemen algılanır ve savunma refleksleri anında devreye girer. Ancak bilişsel harpte yürütülen dekoherans müdahaleleri, sistemin katmanları arasına o kadar derinden entegre edilir ki, hedef kitle bu değişimi dışsal bir operasyon olarak değil;

kendi içinden kaynaklanan organik bir kriz, doğal bir politik kutuplaşma, jenerasyonel bir çatışma veya meşru bir toplumsal itiraz dalgası olarak algılar.4 Sistem, aslında dışarıdan bir düşmanın mühendisliğiyle zehirlendiğini fark etmeksizin kendi kendini paralize eder.

Bu karanlık tablo karşısında sistemlerin hayatta kalabilmesi "transmorfans" (transmorphance) kapasitesine bağlıdır. Geleneksel güvenlik modelleri, bir saldırı sonrası sistemin hasar görüp ardından eski işleyişine dönmesine odaklanan reaktif "dayanıklılık" (resilience) paradigmasına yaslanırken; transmorfans, istikrarsızlık ve belirsizlik koşullarında bile sistemin temel ontolojik çekirdeğini (sistemik invariantlarını) kaybetmeden derin yapısal dönüşümler geçirebilme ve öngörülemez şokları bir gelişim motoru olarak kullanabilme kapasitesini ifade eder.4 Adaptif güvenliğin bu yeni çerçevesi, devletlerin bilişsel güvenliklerini sadece savunma hatları kurarak değil, toplumlarının zihinsel bağışıklığını yapısal olarak evrimleştirerek sağlamaları gerektiğini vurgulamaktadır.

Akademik Teoriler Bilişsel operasyonların karmaşık sosyo-teknik sistemler üzerindeki etkilerini tam anlamıyla analiz edebilmek için, ağ bilimi (network science), kompleks sistemler teorisi, ekolojik modelleme ve ileri düzey veri analizlerinin entegre edildiği multidisipliner akademik teorilere başvurulması zorunludur. Sosyal sistemler, bireylerin ve grupların sadece tek boyutlu ilişkiler kurduğu basit, izole edilmiş yapılar değildir. Aksine, aynı aktörlerin farklı sosyal, ekonomik ve iletişimsel katmanlarda aynı anda etkileşime girdiği son derece karmaşık "çoğullamalı ağlar" (multiplex networks) olarak modellenmeleri gerekir.9 Çoğullamalı ağ teorisi, geleneksel tek katmanlı (single-layer) ağ analizlerinin yetersizliklerini gidermek üzere geliştirilmiştir. Bir çoğullamalı ağ, aynı düğümlerin (nodes - örneğin bireyler, sosyal gruplar, kurumlar) farklı etkileşim türlerini temsil eden iki veya daha fazla katmanda birbirine bağlandığı bir yapıdır.9 Örneğin, bireyler fiziksel mekanda aynı mahallede yaşarken (fiziksel katman), dijital ortamda farklı politik yankı odalarında bulunabilir (enformasyon katmanı) ve ekonomik olarak bir tedarik zincirinin parçası olabilirler.

Literatürde "işaretli ağlar" (signed networks) teorisi, bu ilişkileri pozitif (işbirliği, güven, arkadaşlık) ve negatif (düşmanlık, saldırganlık, güvensizlik) bağlar olarak iki katmana ayırmayı öngörse de, modern bilişsel harp

araştırmaları bu iki katman arasındaki doğrusal olmayan etkileşimi dikkate almanın elzem olduğunu göstermektedir.9 Negatif bağlar ve düşmanlık hissi, ağ içerisindeki bazı düğümlerin merkeziliğini artırarak, ortak bir düşman algısı üzerinden belirli bir alt grubun iç uyumunu radikal biçimde pekiştirebilmektedir.9 Bilişsel kutuplaşma ve fikir dinamiklerinin yayılımı, "SIRQD epidemiyolojik modelleri" ile "q-voter" fikir dinamikleri modellerinin birleştirilmesi yoluyla incelenmektedir.

COVID-19 pandemisinde maske kullanımı ve dijital kutuplaşmanın modellenmesinde başarıyla kullanılan bu entegre akademik yaklaşım, epidemiyolojik bir virüsün yayılımı (Susceptible-Infectious-Recovered-Quarantined-Deceased) ile bir inancın veya fikrin yayılımı arasındaki doğrudan korelasyonu matematiksel olarak ispatlamıştır.11 Çoğullamalı ağlarda bir fikrin benimsenmesi; sadece bireysel bağımsız eylemlere değil, sosyal baskı mekanizmalarına, grup konformizmine ve aralıklı etkiye sahip liderlerin (intermittent-influence leaders) yarattığı manipülatif dalgalanmalara bağlıdır.12 Bu modeller, "çok seviyeli sosyal pekiştirme" (multilevel social reinforcement) adı verilen bir olguyu ortaya koymuştur.

Çok seviyeli pekiştirme, ağ içerisinde "ikili kararlılık" (bistability) durumları yaratarak, yanlış bilginin veya dezenformasyonun bir kez sistemde kök saldıktan sonra, düzeltici karşı önlemler (doğruluk kontrolü, yalanlama) uygulansa dahi ağdan silinmesini imkansızlaştıran dirençli "yok olma ve salgın" (extinction and outbreak) döngülerini açıklamaktadır.13 Kaskad dinamikleri ve bilginin ağlar arası yayılımı, akademik çevrelerde doğrusal eşik modelleri (linear threshold models), simplektik diferansiyel denklem ağları (symplectic ode-net) ve Hamiltonian dinamikleri kullanılarak simüle edilmektedir.14 Bu matematiksel yaklaşımlar, bir dezenformasyon dalgasının ağ üzerinde ne zaman kritik bir eşiği aşarak tüm sistemi sarsacak bir "kaskad" (zincirleme reaksiyon) başlatacağını öngörmeyi amaçlar. Çoğullamalı ağlarda katmanlar arası geçiş maliyeti (layer-crossing overhead) ve bağlantısallık matrisleri (communicability matrix), dış müdahalelerin bir katmandan diğerine sızma kapasitesini ölçer.15

Sistemin tamamının yapısını tek bir düğümden ziyade, katmanlar arası topolojide yer alan zafiyetler belirler.17 Modern araştırmalar ayrıca, bilişsel ağlardaki bağlantı tahminleri (link prediction) ve veri kümeleme (clustering)

problemlerine yönelik devrimsel teknolojilere işaret etmektedir. Sınırlı sosyal ağ verisinden gelecekteki toplumsal kırılmaları tahmin edebilmek için varyasyonel kuantum sınıflandırıcılarına dayanan kuantum destekli yöntemler, bulanık mantık tabanlı bilgi yayılımı (fuzzy-based information diffusion) teknikleri ve zamansal hiper-çizge bellek ağları (temporal hypergraph memory networks) geliştirilmiştir.18 Bunun yanı sıra, karmaşık çok görünümlü (multi-view) verilerin entegrasyonu için geliştirilen ara ve geç entegrasyon (intermediate and late integration) paradigmalarının hibrit kullanımı, düşmanın sosyal ağlardaki bilişsel harp taktiklerini erken evrede kümeleyerek analiz etmek için kritik araçlar sunmaktadır.19

Akademik teoriler, siber güvenliğin fiziksel donanım korumasından ziyade, insan zihninin matematiksel modellere dökülebilen bu çok boyutlu ağ mimarilerinin korunmasına doğru kesin bir eksen kayması yaşadığını göstermektedir.

Sistem Mimarisi Bir toplumun veya kurumun bilişsel olarak ele geçirilmesi ve dekoheransa sürüklenmesi tesadüfi bir süreç değildir; karmaşık sosyo-teknik sistemin temel mimarisinin sistemli bir şekilde sömürülmesini gerektirir. Sistem mimarisi, ontolojik olarak birbirinden farklı özellikler gösteren ancak fonksiyonel olarak birbirine bağımlı üç ana katmandan oluşmaktadır: Bilişsel Katman (Cognition), Fiziksel Katman (Physical) ve Bilgi Katmanı (Information).10 Fiziksel katman, sistemin donanımsal ve coğrafi mevcudiyetidir. Bireylerin fiziksel varlıkları, fiber optik kablolar, sunucular, askeri üsler ve devlet binaları bu katmanda yer alır. Bilgi katmanı, verilerin dijital ve analog formatlarda üretildiği, depolandığı, algoritmalar vasıtasıyla işlendiği ve iletişim kanalları üzerinden hedef kitlelere aktarıldığı teknolojik medya ekosistemidir. Bilişsel katman ise, insan zihninin doğrudan faaliyet gösterdiği; anlamlandırma, hatırlama, problem çözme, koordinasyon, değer yargısı oluşturma ve stratejik karar verme süreçlerinin gerçekleştiği görünmez, soyut ancak sistemin yönetimini sağlayan yegane katmandır.10 Bilişsel harbin tüm stratejik gücü, bu mimari içindeki katmanların birbirine bağlandığı "katmanlar arası topolojiden" (inter-layer topology) gelir.4 Sistemin zafiyet haritası, bir katmandaki sarsıntının diğer katmanlara nasıl aktarıldığına bakılarak çıkartılır. Bu yapıdaki en hayati unsurlar, katmanlar arası geçişi sağlayan "bağlayıcı düğümler"dir (connector nodes). Kanaat

önderleri, büyük medya kuruluşları, bağımsız teyit organizasyonları, adli kurumlar, üniversiteler ve devletin kilit iletişim birimleri birer bağlayıcı düğüm olarak işlev görür.4 Bir bağlayıcı düğüm, örneğin bilgi katmanındaki doğru veriyi süzerek bilişsel katmana güvenilir bir epistemik temel olarak aktarmakla görevlidir. bilişsel harp operasyonlarında düşman aktör, bu düğümleri fiziksel olarak yok etmek yerine onları itibarsızlaştırmaya, ele geçirmeye veya bilgi kirliliği yaratarak nötralize etmeye çalışır.4 Bağlayıcı düğümlerin iflas etmesi, sistemin katmanları arasındaki güvenilir iletişim akışını koparark sistem genelinde bağlantısallığın (connectivity) çökmesine neden olur.

Sistem mimarisine yönelik saldırıların mekaniği, NATO'nun operasyonel araştırmalarına göre üç farklı vektöryel eksende gerçekleşmektedir:

Hedefleme Vektörü Operasyonel Yönelim Etki Mekanizması ve Sistemsel Sonuç

Aşağıdan Yukarıya Biyolojik hedeflerin Beyin-Bilgisayar arayüzleri (Bottom-Up) psikolojik ve sosyal seviyeye ve nöroteknolojilerle yansıması bireylerin otonom sinir sistemlerinde stres ve korku (biyolojik uyarılma) yaratılarak kitlelerde bilişsel esnekliğin yok edilmesi ve sosyo-politik panik başlatılması.20

Merkezden Dışarıya Psikolojik manipülasyon Dijital platformlarda (Middle-Out) üzerinden biyolojik ve oluşturulan yankı odalarında sosyal alanın ele geçirilmesi (echo chambers) mikro-hedeflemeli mesajlarla öfkenin kışkırtılması, bireylerin biyolojik stres seviyesinin artırılması ve bunun sosyal protestolara/çatışmalara dönüştürülmesi.20

Yukarıdan Aşağıya Sosyal/Makro düzeydeki Kurumsal meşruiyetin, (Top-Down) anlatıların mikrodüzeydeki liderliğin ve yasal altyapıların bireyleri kırması makro anlatılarla deforme edilerek, toplumdaki alt grupların ve bireylerin psikolojik aidiyet duygularının, inançlarının ve biyolojik güvenlik hislerinin parçalanması.20

Yapay zekâ (AI) ve makine öğrenmesi araçları, bu üç vektörü de eş zamanlı olarak kullanabilen "hızlandırıcı asimetrik güçler" olarak bu sistem mimarisine sızmaktadır.21 Sistemin bağlayıcı düğümleri işlevini yerine getiremediğinde, toplumun alt parçaları kendi başlarına (yerel olarak)

çalışmaya devam etseler de; makro stratejik kararlar almak ve bütüncül bir duruş sergilemek imkansızlaşır.1

Gerçek Dünya Vakaları

Akademik teoriler ve mimari modeller incelendiğinde, bu konseptlerin uluslararası aktörler tarafından sahada doğrudan uygulamaya konduğu görülmektedir. Askeri ve sivil istihbarat raporları, bilişsel harbin devlet politikalarının merkezine yerleştiği spesifik vakalara işaret etmektedir.

Rusya-Ukrayna Çatışması ve NATO Karşıtı Bilişsel Harekâtlar

Rusya Federasyonu, bilişsel harbi sadece konvansiyonel silahlı bir çatışmanın destekleyici bir unsuru olarak değil; başlı başına bir savaş, bir rejim sürdürme ve bir işgal/yönetişim biçimi olarak benimsemiştir.23 Rus stratejik düşüncesinde savaşlar, cepheden önce düşmanın zihninde ve karar alma organlarında kazanılır veya kaybedilir. Kremlin, yalnızca uluslararası arenada değil, kendi iç kamuoyunda ve işgal ettiği topraklarda istikrarı sağlamak amacıyla sürekli bir bilişsel operasyon yürütmektedir.23 Ukrayna işgali sürecinde Rusya, "bilgi süper gücü" (information superpower) kapasitesini kullanarak hedef toplumların epistemik ve teleolojik invariantlarına yönelmiştir.24 Operasyonların temel mekanizması; nükleer savaş tehdidi, anti-NATO söylemleri ve kurbanlaştırma (victimization) anlatıları üzerinden korku ve belirsizlik duygularının sistematik olarak topluma zerk edilmesidir.25 Araştırmalar, dezenformasyon dalgalarının rastgele olmadığını, doğrudan önemli jeopolitik gelişmelerle (örneğin NATO zirveleri) senkronize edildiğini göstermektedir.25 Batılı toplumların ve Ukrayna vatandaşlarının kurumlara olan güvenini yıkmak amacıyla hazırlanan deepfake içerikleri, NATO'nun egemenlik ihlalleri yaptığına dair sahte anlatılarla birleştirilerek, hedeflerin rasyonel analiz süreçlerini by-pass edip doğrudan duygusal salience (belirginlik) üzerinden bilinçaltı manipülasyon yaratmayı amaçlamıştır.25 Rusya, doğrudan askeri olarak ezemediği rakibini, kendi içinde şüpheye düşürerek karar alma felci (reflexive control) yaşamaya zorlamaktadır.27 **Çin Halk Cumhuriyeti: Üç Harp Doktrini ve Tayvan Kuşatması**

Çin'in stratejik kültürü, "savaşmadan kazanmayı" en yüksek askeri ideal olarak tanımlayan Sun Tzu ekolüne dayanır ve bu felsefe günümüzde "bilişsel hakimiyet" (cognitive dominance) ve "zeka hakimiyeti" (intelligence

dominance) konseptleriyle modernize edilmiştir.28 Çin Halk Kurtuluş Ordusu'nun (PLA) Siyasi İşler Departmanı tarafından yönetilen "Üç Harp" (San Zhong Zhanfa / Three Warfares) doktrini, modern bilişsel harpın Asya-Pasifik'teki en yapısal örneğidir.28 Üç Harp doktrini şu alt operasyonlardan oluşur:

1. Kamuoyu Savaşı (Public Opinion Warfare): Çin'in ulusal çıkarları doğrultusunda hem iç hem de küresel ölçekteki medya ekosistemini ve enformasyon akışını domine etme faaliyetleri.

2. Psikolojik Savaş (Psychological Warfare): Düşman askerlerinin ve sivil halkın moralini, savaşma iradesini ve liderliğe olan güvenini çökertmeye yönelik sindirme operasyonları.

3. Hukuk Savaşı (Legal Warfare - Lawfare): Mevcut uluslararası hukuku manipüle ederek veya yeni hukuki standartlar dayatarak Çin'in gri bölge faaliyetlerine ve asimetrik askeri operasyonlarına yasal bir meşruiyet kalkanı yaratılması.28 RAND ve CSIS raporlarına göre Çin'in Amerika Birleşik Devletleri'ne yönelik bilişsel harp operasyonlarında uyguladığı "ağ sömürüsü", doğrudan kimliksel invariantları hedef almaktadır.

Olası bir çatışmada Çin'in ilk hedeflerinden biri, ABD ordusunda görev yapan etnik Çinli subaylar, askerler ve onların aile ağlarıdır.30 Dezenformasyon ve duygusal şantaj mekanizmalarıyla bu personelin ABD'ye olan sadakat bağları zayıflatılmaya çalışılmaktadır; nitekim 2023 yılında Çin istihbaratına casusluk yaparken yakalanan iki ABD donanma askerinin, Çin vatandaşı anneleri üzerinden manipüle edildiği tespit edilmiştir.30 Tayvan bağlamında ise Çin, "bilişsel aşırı yükleme" (cognitive overload) taktiklerini kullanmaktadır. Uçakların ve donanma gemilerinin ada etrafında bitmek bilmeyen askeri manevraları, hedeflenen siber saldırılar ve beyin hedefleme (brain targeting) pratikleriyle birleştirilerek, Tayvan halkı sürekli bir psikolojik aşınmaya maruz bırakılmaktadır.31 Beyin-bilgisayar arayüzü (BCI) bağlantılı nörometrik veriler kullanılarak kitlelerin tepkileri ölçülmekte ve Tayvan'ın sosyal yapısı, kurumları ve direnç eksenleri felç edilmeye çalışılmaktadır.32 Avrupa'nın Enerji Dönüşümünde Jeoekonomik Operasyonlar

Bilişsel harp sadece askeri aktörler arasında değil, makro-ekonomik çıkarlar ekseninde jeoekonomik bir silah olarak da kullanılmaktadır. Avrupa Birliği'nin fosil yakıtlardan çıkış hedeflerini içeren **"Avrupa Yeşil Mutabakatı" (European Green Deal)** süreçlerinde yaşananlar, bilgi kontrolünün ve siber manipülasyonun stratejik düzeyde nasıl kullanıldığını göstermektedir.33 Devlet ve devlet dışı aktörler, Avrupa'nın yenilenebilir enerji ile nükleer enerji arasındaki regülatif tartışmalarına sosyal medya platformlarındaki algoritmik amplifikasyon taktikleriyle dahil olmuşlardır.33 Bu operasyonlarda temel hedef, toplumun çevresel güven ve enerji güvenliği konusundaki aksiyolojik değer yargılarını birbirine çarptırarak felç etmektir. Demokratik sistemlerin temel değerleri olan ifade özgürlüğü (ECHR Madde 10) ile bilgi güvenliği (AI Act, AB Dijital Savunma yasaları) arasındaki yasal boşluklar "hibrit tehdit aktörleri" tarafından ustalıkla sömürülerek 33, sadece bir enerji politikasının değil, Avrupa entegrasyonu vizyonunun (teleolojik invariant) sekteye uğratılması hedeflenmiştir.

Mekanizma Analizi Gerçek dünya vakalarında gözlemlenen dekoherans tablosu, çoğullamalı ağ mimarilerinde belirli bir kaskad (zincirleme) algoritması takip edilerek inşa edilmektedir. Sistemik bir invarianta yönelik başarılı bir saldırının, sosyo-teknik yapının tamamını nasıl çökerttiği dört aşamalı bir mekanizma olarak incelenebilir:

1. Epistemik Erozyon ve Bağlayıcı Düğümün (Connector Node) İmhası: Bilişsel operasyon genellikle sınırlı ve yüksek hassasiyetli bir sızma ile başlar. Sistemin epistemik güvenliğinin belkemiği olan bir otorite (örneğin ülkenin seçim kurumu, yüksek yargısı veya ulusal sağlık enstitüsü), yapay zekâ tarafından üretilmiş sızdırılmış sahte belgeler veya deepfake videolarıyla itibarsızlaştırılır.4 Sistemin gerçekliği doğrulama kapasitesi ilk darbeyi alır.

2. Aksiyolojik ve Sosyal Aşınmanın Yayılımı: Epistemik katmandaki sarsıntı, çoğullamalı ağın çapraz katman bağlantıları üzerinden değerler (aksiyolojik) ve sosyal güven katmanına sıçrar. Ortak bir "doğru" kavramının kaybolması, toplumdaki alt grupların her birinin kendi alternatif gerçekliğini üretmesine yol açar.4 Bu süreçte karar alıcılar, uyumsuz alternatifler arasında kaotik salınımlar göstererek "karar alma paralizasyonu" (paralysis of decision-making) yaşarlar.4

3. Kimliksel Parçalanma ve Kutuplaşma: Makro düzeydeki kurumsal güvenin çökmesiyle birlikte sistemin üyeleri, psikolojik bir savunma refleksi olarak mikro-kimliklere ve daha dar çerçeveli sadakat gruplarına sığınırlar. İnsan doğasındaki sosyal aidiyet ihtiyacı ve bilişsel katılık (cognitive inflexibility) özellikleri sömürülerek, gruplar arası diyalog tamamen koparılır.27 Bu aşamada "negatif bağlar" sistemi domine eder, gruplar sadece ortak düşmanlıklarda birleşir.9

4. Teleolojik Çöküş ve Bilişsel Dekoheransın Tamamlanması: Tarihsel geçmişi ve mevcut gerçekliği konusunda uzlaşamayan ve birbirine düşman gruplara ayrılan bir sosyo-teknik sistemin ortak bir gelecek vizyonu belirleme yeteneği ortadan kalkar.4 Düşman dışarıdan tek bir kurşun atmadan, hedef sistemi kendi kendini yok eden, enerjisini kendi iç çatışmalarında tüketen bağımlı bir yapıya dönüştürür.

Bu yıkıcı mekanizmayı hızlandıran en önemli unsur **"Üretken Yapay Zekâ" (Generative AI)** ve nöroteknolojilerin birleşimidir.20 2025 yılı sonlarında NATO Müttefik Dönüşüm Komutanlığı (ACT) ve NATO İletişim ve Bilgi Ajansı (NCIA) himayesinde "Reality Defender" şirketi tarafından yürütülen özel bir deney, bu araçların taktiksel değil "operasyonel" tehdit seviyesini açıkça kanıtlamıştır.34 Senaryo kapsamında, tecrübeli askeri planlayıcıların (operational planners) görev yaptığı bir harp oyununda karar alıcılara kontrollü olarak gelişmiş deepfake içerikler sunulmuştur.34 Deneyin sonuçları son derece çarpıcıdır: En deneyimli personelin dahi bilişsel aşırı yüklenme (cognitive overload) yaşadığı, operasyonel hızın sekteye uğradığı ve rakip tarafından oluşturulan "kurgusal gerçekliklerin" (false realities) kararları doğrudan saptırdığı saptanmıştır.34

Trend Analizi (2020–2026) bilişsel harp teorilerinin ve asimetrik mücadele pratiklerinin son altı yıllık evrimi, alanın salt bir teorik tartışma olmaktan çıkıp, uluslararası ittifakların acil müdahale gerektiren doktriner merkezine oturduğunu göstermektedir.

2020–2021: Bilişsel Alanın Bağımsız Bir Harp Ortamı Olarak Tanınması Yapay zekâ ve büyük veri analitiğinin sosyal medya algoritmalarını tamamen otomatikleştirmesiyle, geleneksel Psikolojik Harekat (PSYOPS) yetersiz kalmıştır. 2021 yılında NATO, "Warfighting Capstone Concept" belgesini yayımlayarak bilişsel alanı, kara, deniz, hava, uzay ve siber

alanların yanında meşru ve kritik bir operasyon sahası olarak resmen tanımış, müttefiklerin bu alanda hem savunma hem de taarruz yetenekleri geliştirmesi gerektiğini vurgulamıştır.22 2022–2023: Ukrayna Savaşı Katalizörü ve Kurumsal Önceliklendirme Rusya'nın Ukrayna'yı geniş çaplı işgali ile birlikte bilişsel harp, tüm şiddetiyle sahaya inmiştir.23 Hibrit tehditlerin demokratik toplumların istikrarı üzerindeki yıkıcı etkileri görülünce, NATO Bilim ve Teknoloji Kurulu (STB) 2022 yılında bilişsel harbi birincil stratejik araştırma alanı (strategic research challenge) ilan etmiştir.22 Eş zamanlı olarak Avrupa Birliği "Horizon Europe" AR-GE fonlarını doğrudan enformasyonun silahlaştırılmasına karşı koymaya ve toplumların dijital manipülasyonları tespit etme kapasitesini artırmaya yönlendirmiştir.21 Çin'in Tayvan etrafındaki provokasyonlarının da artmasıyla "gri bölge" çatışmaları askeri norm haline gelmiştir.

2024–2025: Yapay Zekâ Hukuku, Operasyonel Deneyler ve Stratejik Uyanış Generative AI araçlarının yaygınlaşmasıyla birlikte dezenformasyonun üretim maliyeti sıfıra yaklaşmış, kalitesi ise insan gözünün ayırt edemeyeceği seviyeye ulaşmıştır.36 Haziran 2024'te yayımlanan AB Yapay Zekâ Yasası (AI Act), ifade özgürlüğü ile platform manipülasyonlarına karşı dijital güvenlik arasındaki yasal çatışmaları çözme yönünde devasa bir adım olmuştur.33 2025 yılında yayımlanan NATO Baş Bilim İnsanı raporu, çatışmaların tamamen "davranış merkezli" (behavior-centric) hale geldiğini vurgulamış; askeri operasyonların ölçütünün mesaj penetrasyonundan, düşmanın davranış eğilimlerindeki kalıcı değişimlere (durable changes) doğru evrildiğini deklare etmiştir.20 Aynı yıl yapılan ACT deepfake deneyleri, komuta-kontrol kademelerinin kırılganlığını kanıtlamıştır.34 2026: Ontolojik Mimari, Tam Olgunlaşma ve Küresel Çözümler Bu stratejik evrimin zirvesi, 2026 yılı içerisinde CCDCOE tarafından yayımlanan "Ontological Foundations of Cognitive Warfare" çalışması ile kaydedilmiştir.3 Silahlı kuvvetlerin ve politika yapıcıların salt dezenformasyona tepki veren (reaktif) yapılar olmaktan çıkıp, sistemik invariantları korumaya yönelik proaktif (transmorfans odaklı) bir mimari geliştirmeleri gerektiği bilimsel bir konsensüse dönüşmüştür.6 Tallinn'de gerçekleştirilen "CyCon 2026: Securing Tomorrow" konferansında küresel uzmanların ele aldığı hukuki ve stratejik boyutlar, bilişsel güvenliğin artık

taktiksel bir destek unsuru değil, varoluşsal bir güvenlik parametresi olduğunu netleştirmiştir.37

Yıl / Dönem Belirleyici Stratejik Evrimsel Taktik ve Doktrin ve Gelişme Odak Noktası Kurumsal Çıktılar

2020-2021 Sosyal İzole bilgi NATO 2021 algoritmaların operasyonlarından Warfighting manipülasyonu, davranış Capstone Concept asimetrik araçların mühendisliğine ile bilişsel sahanın tırmanışı. geçiş. resmen tanınması.

2022-2023 Rusya'nın Ukrayna Yankı odalarında NATO STB işgali; nükleer korku hedefli panik; önceliklendirmesi yayılımı, Çin'in sınır kurumsal güven (2022); EU Horizon tacizleri. yıkımı (epistemik fonlarının dijital erozyon). esnekliğe ayrılması.

2024-2025 Üretken YZ'nin Nöroteknolojik EU AI Act (2024); tabana inmesi, karar verilerin (BCI) NATO ACT 2025 alıcıların doğrudan kullanımı, Operasyonel hedef alınması. operasyonel Deepfake dekoherans Deneyleri; NATO yaratma. Baş Bilim İnsanı Raporu (2025).

2026 "Sürekli savaş alanı" Çoğullamalı ağların CCDCOE "Bilişsel paradigması, (multiplex) Harbin Ontolojik sistemik sömürülmesi, Temelleri" invariantlara yönelik Transmorfans Araştırması; CyCon ontolojik yaklaşım. kapasitesi tesisi. 2026 Siber İhtilaflar Konferansı.

Stratejik Sonuçlar Sunulan bu derinlemesine akademik, askeri ve operasyonel analizin neticesinde, sosyo-teknik sistemlerin güvenliğini tesis etmekle yükümlü olan devlet organları, güvenlik ittifakları ve stratejik karar alıcılar için hayati sonuçlar ortaya çıkmaktadır. Düşmanın savaş konsepti değiştiği için, ulusal savunmanın başarı ölçütleri (MoE) ve savunma yöntemleri radikal bir yapısal revizyona tabi tutulmalıdır.20

1. "Tüm Ulus" (Whole-of-Nation) ve Çok Katmanlı Güvenlik Yaklaşımı: Bilişsel harp stratejileriyle mücadele salt ordu, siber güvenlik merkezleri veya istihbarat örgütlerinin inisiyatifine bırakılamaz.32 Sosyal sistemlerin çoğullamalı ağ mimarisinde yer alan sistemik invariantların korunması; sivil otoritenin, eğitim kurumlarının, üniversitelerin, medya organizasyonlarının, yargı mensuplarının ve sivil toplum örgütlerinin tam entegrasyonunu gerektirir.32 Sistem içerisindeki "bağlayıcı düğümler" (connector nodes) haritalandırılmalı ve bu kişi/kurumların epistemik

otoritelerini dezenformasyon saldırılarına karşı yasal ve teknolojik olarak koruyacak zırhlar (media literacy programs, fact-checking altyapıları) oluşturulmalıdır.4 Kötü niyetli faaliyetlerin anında ifşa edilerek kaynağının hızla tespit edilmesi (rapid attribution), caydırıcılık stratejisinin merkezinde yer almalıdır.32

2. Askeri Eğitim ve Karar Alma Organlarının Bilişsel Zırhlanması: NATO ACT 2025 deneylerinin kanıtladığı üzere, en kıdemli askeri ve bürokratik planlayıcılar dahi hiper-gerçekçi yapay zekâ operasyonlarının tehdidi altındadır.34 Bu bağlamda personel eğitimi sadece fiziksel dayanıklılık veya konvansiyonel siber hijyeni değil, yapısal bir "bilişsel esneklik" (cognitive flexibility) kazanımını içermelidir.27 Bireylerin tehlikeli boyuttaki duygusal uyarılmalarını (emotional arousal) minimize eden, grup kutuplaşmalarını törpüleyen, şüpheci ve analitik sorgulamayı kurumsallaştıran yeni nesil eğitim doktrinleri acilen devreye alınmalıdır.27 Askeri görevlerde Başarı Ölçütü (Measure of Effectiveness - MoE) artık sadece bir mesajın hedefe ulaşması değil, hedefteki kitlenin dayanıklılığının, bağlılık hissinin ve kurumsal meşruiyet algısının kalıcı (durable) olarak ayakta tutulabilmesidir.20

3. Müttefik İşbirliği ve Ortak Transmorfans Kapasitesinin Geliştirilmesi: Küresel olarak birbirine bağımlı dünyada hiçbir ülke, sınıraşan bilişsel operasyonlarla tek başına başa çıkamaz.

Stratejik hedef, ulusal sınırları bilgi sızıntısına kapatmak değil (ki bu imkansızdır); sistemin öngörülemez yalanlar karşısında dahi temel invariantlarını koruyarak organik bir evrim geçirebilme (transmorphance) kapasitesini inşa etmektir.6 Bu yönde, yapay zekâ araçlarının dezenformasyon saptamada pozitif bir kalkan olarak kullanılması için çok uluslu veri paylaşım mekanizmaları oluşturulmalıdır.36 Ayrıca, Güvenlik Gücü Yardımı (SFA) gibi uluslararası ortaklık faaliyetleri, yalnızca askeri personeli eğitmekle kalmamalı, ev sahibi ülkelerin kritik teknolojik altyapılarının ve dijital dirençlerinin gelişimini kapsayacak şekilde genişletilmelidir.39 Sosyal sistemlerin epistemik çerçevelerini, güven mimarilerini ve ortak aidiyet duygularını hedef alan modern bilişsel harp, geçici bir asimetrik taktik değil; uluslararası güç mücadelesinin kalıcı ve görünmez bir boyutudur. Devletlerin ve kurumların bekası, konvansiyonel

silah depolarının büyüklüğüne değil; toplumlarının anlamlandırma kapasitelerini, çoğullamalı algı ağlarını ve gerçeğe dair sarsılmaz inançlarını "dekoherans" girdabına karşı ne ölçüde koruyabileceklerine bağlı olacaktır.

Alıntılanan çalışmalar

1. New CCDCOE research reconceptualises cognitive warfare, erişim tarihi Haziran 3, 2026, https://ccdcoe.org/news/2026/new-ccdcoe-research-reconceptualises-cognitive -warfare/

2. Invisible by design: NATO's 2026 cognitive warfare paper and the..., erişim tarihi Haziran 3, 2026, https://complexdiscovery.com/invisible-by-design-natos-2026-cognitive-warfare -paper-and-the-crisis-of-discovery/

3. Ontological Foundations of Cognitive Warfare - CCDCOE, erişim tarihi Haziran 3, 2026, https://ccdcoe.org/library/publications/ontological-foundations-of-cognitive-warf are

4. Ontological Foundations of Cognitive Warfare - CCDCOE, erişim tarihi Haziran 3, 2026, https://ccdcoe.org/uploads/2026/04/ONTOLOGICAL_FOUNDATIONS_OF_COGNI TIVE_WARFARE.pdf

5. China's 'Three Warfares': Origins, Applications, and Organizations - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/262583765_China's_'Three_Warfares'_O rigins_Applications_and_Organizations

6. (PDF) Adaptive security: strategic principles for complex socio-technical systems, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/399950891_Adaptive_security_strategi c_principles_for_complex_socio-technical_systems

7. (PDF) How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/362163528_How_China's_Cognitive_Wa rfare_Works_A_Frontline_Perspective_of_Taiwan's_Anti-Disinformation_Wars

8. (PDF) Cognitive warfare - the human mind as the new battlefield - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/391704397_Cognitive_warfare_-_the_h uman_mind_as_the_new_battlefield

9. Signed Networks: theory, methods, and applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2511.17247v2

10.AI-enhanced collective intelligence - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2403.10433v4

11. Role of Time Scales in the Coupled Epidemic-Opinion Dynamics on Multiplex Networks, erişim tarihi Haziran 3, 2026, https://www.mdpi.com/1099-4300/24/1/105

12.The Structure and Function of Complex Networks | SIAM Review, erişim tarihi Haziran 3, 2026, https://epubs.siam.org/doi/10.1137/s003614450342480

13.Emergent Dynamics in Multiplex Social Networks: Agent-Based Modeling of Information Diffusion for Misinformation Control - The Open Repository @ Binghamton (The ORB), erişim tarihi Haziran 3, 2026, https://orb.binghamton.edu/cgi/viewcontent.cgi?article=1152&context=nejcs

14.Model-based Investigation of Cascade Dynamics on Multi-layer Networks - Leonard Lab - Princeton University, erişim tarihi Haziran 3, 2026, https://naomi.princeton.edu/wp-content/uploads/sites/744/2021/01/Desmond_Ph D_Thesis_ProQuest.pdf

15.Dynamical processes and emergent behaviors in multiplex networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2605.04199v1

16.Spreading processes in Multilayer Networks - Unibo, erişim tarihi Haziran 3, 2026, http://www.cs.unibo.it/~montesi/CBD/Articoli/Spreading%20processes%20in%20 Multilayer%20Networks.pdf

17.The structure and dynamics of multiplex networks - QMRO, erişim tarihi Haziran 3, 2026,

https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/30631/BATTISTON_Fe derico_PhD_Final_041017.pdf

18.Leveraging similarity and community-based features for link prediction in temporal social networks using attention-enabled LSTM - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12753736/

19.Multi-View Clustering of Social-Based Data - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1157337.pdf

20.Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness > Institute for National Strategic Studies > View Publications, erişim tarihi Haziran 3, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/43711 95/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-ope rat/

21.EMERGING DISRUPTIVE TECHNOLOGIES and TERRORISM - COE-DAT, erişim tarihi Haziran 3, 2026, https://www.tmmm.tsk.tr/publication/researches/24-Emerging_Disruptive_Technol ogiesandTerrorism.pdf

22.Cognitive warfare: NATO chief scientist research report, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-wa rfare-final.pdf

23.A Primer on Russian Cognitive Warfare | ISW, erişim tarihi Haziran 3, 2026, https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-co gnitive-warfare/

24.The Cognitive Campaign: - Strategic and Intelligence Perspectives - INSS, erişim tarihi Haziran 3, 2026, https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pd f

25.Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12460417/

26.Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine - RAND Corporation, erişim tarihi Haziran 3, 2026,

https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3400/RRA34 00-1/RAND_RRA3400-1.pdf

27.The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and Bridging the Gap to Extant Literatures - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO %20Meeting%20Proceedings/ST O-MP-HFM-361/MP-HFM-361-P13.pdf

28.Assessing “Cognitive Warfare”, erişim tarihi Haziran 3, 2026, https://irregularwarfare.org/articles/assessing-cognitive-warfare/

29.China's Quest for Control of the Cognitive Domain and Gray Zone Situations, erişim tarihi Haziran 3, 2026, https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_20 23_A01_revised.pdf

30.Chinas Second Battlefield - Marine Corps University, erişim tarihi Haziran 3, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/J AMS-vol-15-no-2/Chinas-Second-Battlefield/

31.Chinese Disinformation Efforts on Social Media - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z 3/RAND_RR4373z3.pdf

32.2026 - Cognitive Warfare by China and India's Response, erişim tarihi Haziran 3, 2026, https://usiofindia.org/pdf/Monograph_no_3.pdf

33.Cognitive Warfare, Disinformation, and Corporate Influence in Europe's Energy Transition: Information Control, Regulation, and Human Rights Implications, erişim tarihi Haziran 3, 2026, https://www.acigjournal.com/Cognitive-Warfare-Disinformation-and-Corporate-I nfluence-in-Europe-s-Energy-nTransition,214045,0,2.html

34.Building Decision-Making Advantage - Integrating Deepfake Insights into NATO experimentation - Reality Defender, erişim tarihi Haziran 3, 2026, https://www.realitydefender.com/insights/reality-defender-joins-nato--cognitive- warfare-experimentation

35.Cognitive Warfare: Generative AI, False Realities, and International Humanitarian Law, erişim tarihi Haziran 3, 2026,

https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1156&conte xt=research

36.The Future of Indo-Pacific Information Warfare - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA2205-1.html

37.CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise., erişim tarihi Haziran 3, 2026, https://ccdcoe.org/

38.Aspects of Cognitive Warfare - The Defence Horizon Journal, erişim tarihi Haziran 3, 2026, https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-W arfare-2024_web-v2.pdf

39.out thinking - on nato 2022 strategic concept, erişim tarihi Haziran 3, 2026, https://www.nsfacoe.org/wp-content/uploads/2024/02/OUT-THINKING-ON-NAT O-STRATEGIC-CONCEPT-Study-Paper.pdf

Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken sistemik invariantlar yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası epistemik yapı, değer hiyerarşisi, kolektif kimlik, sosyal güven ve ortak gelecek tasavvuru üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir. Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar. Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle sistemik invariantlar alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?
  - Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi?
  - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?
  - YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı

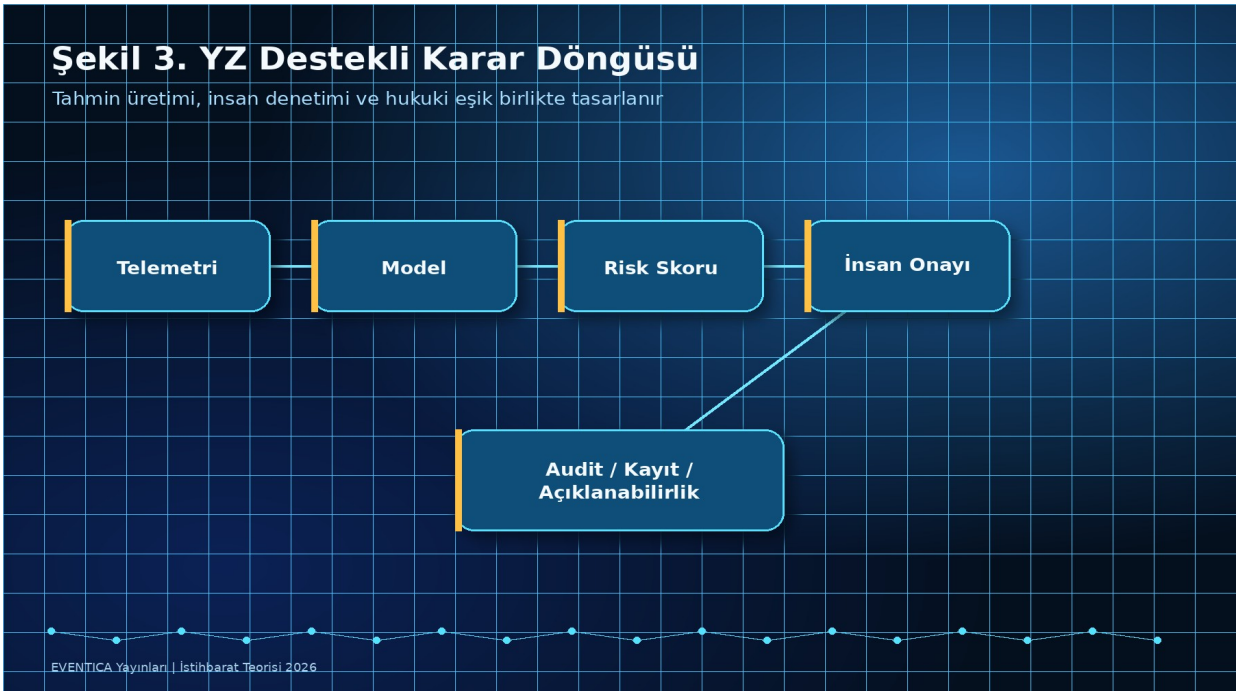
mı?
- Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?
- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı?
- Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Sistemik İnvariantlar ve Sosyal Sistemlerin Hedef Alınması alanında en güçlü erken uyarı göstergeleri hangileridir?
2. Bu göstergeler hangi durumda yanlış pozitif üretir?
3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?
4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma sağlanmalıdır?
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı anlamlara gelir?
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?
8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 3. Yapay Zekâ Destekli Tahmin Sistemleri ve Makine Hızında Karar Alma

Makine hızı karar üstünlüğü sağlayabilir; ama stratejik bağlamdan koparsa hızlı hata üretir. Bu bölüm hız, kontrol ve anlamlı insan denetimi arasındaki gerilimi inceler.



Şekil 4. Makine hızında karar mimarisinde hız ve doğruluk gerilimi

Tablo 6. YZ tahmin sistemlerinde ana risk alanları

Risk	Açıklama	Kontrol sorusu
Model yanlılığı	Eğitim verisinin temsil gücü sınırlı olabilir	Model hangi veriyi görmedi?
Aşırı güven	Skor yüksek görünse de bağlam eksik olabilir	Güven seviyesi nasıl hesaplandı?
Stratejik sağırlık	Taktik başarı stratejik hedefi bozabilir	Model politik sonucu anlıyor mu?
İnsan dışlama	Operatör sadece onay makamına dönüşebilir	Anlamlı insan kontrolü korunuyor mu?

Bölüm 3: Yapay Zekâ Destekli Tahmin

Sistemleri: Pekiştirmeli Öğrenme ve Makine Hızında Karar Alma Algoritmaları Modern harp sahası, bilginin, verinin ve reaksiyon hızının

benzersiz bir hacimde birleştiği, geleneksel komuta kontrol mekanizmalarının ve insan bilişinin sınırlarının yapısal olarak yetersiz kaldığı yeni bir teknolojik döneme girmiştir. İçinde bulunduğumuz bu çağda, stratejik üstünlük salt ateş gücü, zırh kalınlığı veya personel sayısıyla değil; devasa veri yığınlarını anlama, bu verilerden anlamlı sonuçlar çıkarma, düşman hareketlerini önceden tahmin etme ve makine hızında (machine-speed) reaksiyon gösterme yeteneğiyle tanımlanmaktadır.1 Bu bağlamda, askeri operasyonlarda yapay zekâ destekli tahmin sistemleri, özellikle pekiştirmeli öğrenme (Reinforcement Learning - RL) ve otonom karar alma algoritmaları, sadece operasyonel birer araç olmaktan çıkarak ulusal güvenlik, caydırıcılık mimarisi ve kuvvet projeksiyonunun mutlak merkezine yerleşmiştir.2 NATO Bilim ve Teknoloji Organizasyonu'nun (STO) IST-173 görev gücü tarafından yayımlanan belgelerde ve geliştirilen misyon odaklı araştırma yol haritalarında "Sentor (Centaur)" yaklaşımıyla vurgulandığı üzere; temel amaç insan yargısını tamamen ortadan kaldırarak makineleri kendi başlarına bırakmak değil, makine hızı ve gücüyle savaşırken anlamlı insan kontrolünü, etik çerçeveyi ve stratejik bağlamı korumaktır.4 İnsan bilişi, aynı anda binlerce değişkenin hesaplanmasını gerektiren çok alanlı operasyonlarda (Multi-Domain Operations - MDO) yetersiz kalırken, pekiştirmeli öğrenme algoritmaları bu karmaşıklığı saniyeler içinde çözebilmektedir. Ancak yapay zekâ modelleri taktiksel olarak kusursuz manevralar üretebilse de, stratejik olarak naif kalma eğilimindedir; bu sistemler düşmanın karar döngüsünün içine sızarak yerel galibiyetler elde edebilir, ancak savaşın genel siyasi ve diplomatik hedeflerini anlama konusunda insan rehberliğine muhtaçtır.6 Bu rapor, algoritmik savaşın ve makine hızında karar alma mekanizmalarının doktrinel evrimini, temelindeki akademik ve matematiksel teorileri, sistem mimarilerini, gerçek dünya vakalarını ve 2020-2026 ufku itibarıyla yaratacağı stratejik sonuçları son derece kapsamlı ve analitik bir perspektifle incelemektedir.

1. Kavramsal Çerçeve Yapay zekâ destekli savaş mimarisinin kavramsal temeli "Algoritmik Savaş" (Algorithmic Warfare) ve "Makine Hızı" (Machine-Speed) paradigmaları etrafında şekillenmektedir. Geleneksel savaş doktrinlerinde strateji ve taktiksel uygulama, komuta kademesinin bilişsel

kapasitesi, kurmay subayların veri işleme hızı ve bürokratik hiyerarşinin getirdiği iletişim gecikmeleriyle sınırlıdır.

Makine hızında karar alma ise, algılayıcı (sensör) ağlarından gelen terabaytlarca verinin anında işlenerek ateşleyici (shooter) unsurlara insan aracılığı olmadan veya onay mekanizmasının saniyenin kesirlerine indirildiği bir hızda iletilmesini ifade eder.7 Bu paradigma, devlet yönetiminin ve stratejinin temel doğasını değiştirmemekle birlikte (devletler hala diplomasi, ekonomik baskı ve askeri güç unsurlarını bir arada kullanmaktadır), savaşın karakterini ve operasyonel temposunu geri döndürülemez biçimde dönüştürmektedir.2

1.1. OODA Döngüsünün Yapısal Dönüşümü

Askeri stratejist John Boyd tarafından kavramsallaştırılan ve yıllarca askeri doktrinlerin temelini oluşturan OODA (Gözlem, Yönelim, Karar, Eylem - Observe, Orient, Decide, Act) döngüsü, pekiştirmeli öğrenme ve tahmin edici algoritmaların entegrasyonu ile radikal bir dönüşüm geçirmektedir. Geleneksel modelde bu dört aşama doğrusal ve ardışıktır; komutan önce sahayı gözlemler, elindeki verilerle durumu yönlendirir, bir karar verir ve ardından eyleme geçer. Bu döngü ne kadar hızlı tamamlanırsa, düşmanın OODA döngüsü o kadar çabuk kırılır ve inisiyatif ele geçirilir.

Ancak DARPA'nın "Deep Green" projesi gibi ileri düzey inisiyatiflerin kavramsallaştırdığı yeni yapıda, OODA döngüsü doğrusal bir süreç olmaktan çıkıp sürekli ve eşzamanlı bir mekanizmaya dönüşmektedir.8 Bu yeni modelde döngü ikiye ayrılmaktadır: Sürekli Gözlem ve Yönelim (OO-döngüsü) ile Özelleştirilmiş Karar ve Eylem (DA-döngüsü). Algoritmalar, sahadaki operasyon devam ederken "Gözlem" ve "Yönelim" aşamalarını sürekli olarak arka planda çalıştırır. Sistem, düşmanın mevcut hareketlerini değerlendirerek savaşın alabileceği binlerce farklı rotayı pekiştirmeli öğrenme simülasyonlarıyla test eder ve gelecekteki olası durumları tahmin eder.9 Böylece komutanın karşısına bir kriz anında sıfırdan plan yapma zorunluluğu çıkmaz; sistem, düşman daha ne yapacağına karar vermeden dost kuvvetlere hazır, optimize edilmiş ve önceden simüle edilmiş eylem planları (Course of Action - CoA) sunar.10 Bu durum, karar alma mekanizmasını reaktif bir süreçten proaktif ve tahmine dayalı bir yapıya yükseltir.

1.2. YZ-Etkinleştirilmiş Sistemlerden YZ-Merkezli Komuta Kontrole Geçiş

Modern askeri doktrinde komuta kontrol mekanizmaları "YZ-etkin" (AI-enabled) olmaktan çıkıp tam anlamıyla "YZ-merkezli" (AI-centric) olmaya doğru evrilmektedir.7 YZ-etkin sistemlerde yapay zekâ, tıpkı gelişmiş bir radar veya gece görüş dürbünü gibi belirli insan görevlerini destekleyen izole, dar kapsamlı bir araçtır. Ancak YZ-merkezli bir yaklaşımda YZ, tüm komuta mimarisinin sinir sistemi olarak görev yapar.7 Bu kavramsal sıçrama, "YZ Ajan Ağı" (AI Agent Mesh) adı verilen bir yapıyla somutlaşmaktadır.

YZ Ajan Ağı, tek bir merkezi sunucu veya devasa bir süper bilgisayar programı değildir; aksine, muharebe sahasının tüm derinliğine yayılmış, kendi kendini organize eden uçtan uca bir otonom ajanlar şebekesidir.7 Bu çerçevede en düşük taktiksel seviyedeki bir insansız hava aracının sensöründen, platform seviyesindeki zırhlı komuta araçlarına ve operasyonel karargahlara kadar her düğüm kendi spesifik YZ ajanlarıyla donatılmıştır.7 Bu ajanlar, insan hiyerarşisinin gerektirdiği dikey raporlama zincirlerini beklemeden yatay eksende birbirleriyle otonom olarak müzakere eder, veri alışverişinde bulunur ve ortak zeka (collective intelligence) oluşturur.7

Karşılaştırma Kriteri Geleneksel Komuta YZ-Merkezli Ajan Ağı (AI Kontrol Agent Mesh)

Bilgi Akışı Dikey ve Sıralı (Hiyerarşik) Yatay, Çok Yönlü ve Eşzamanlı

Karar Mercii Kurmay Heyeti ve İnsan Yerel otonom ajanlar ve Komutan insan gözetimi

Veri İşleme Konumu Merkezi Karargah (Veri Uçta İşleme (Edge merkeze taşınır) Computing)

Hedef Tahsisi Süresi Dakikalar / Saatler Milisaniyeler / Saniyeler

Ölçeklenebilirlik İnsan bilişi ve yorgunlukla Ağa eklenen her sensörle sınırlı logaritmik artış

1.3. Ölüm Zincirinden Ölüm Ağına Paradigma Değişimi (Kill Chain vs. Kill Web)

Uzun yıllar boyunca ordular askeri hedeflerin yok edilmesini bir "Ölüm Zinciri" (Kill Chain) modeliyle tasarlamıştır. Zincir metaforu, sürecin doğrusallığını vurgular: Hedefi bul, sabitle, takip et, hedefle, angaje ol ve değerlendir (F2T2EA). Ancak doğrusal zincirler kırılgandır; iletişim rölesinin vurulması, radarı körelten bir elektronik harp saldırısı veya bir kurmay subayın yorgunluktan hata yapması tüm zincirin çökmesine ve hedefin kaçırılmasına neden olabilir.

Günümüzde ABD Savunma Bakanlığı tarafından JADC2 (Joint All-Domain Command and Control) ve DARPA'nın ACK (Adapting Cross-Domain Kill-webs) programları kapsamında geliştirilen "Ölüm Ağı" (Kill Web) konsepti bu kırılganlığı ortadan kaldırmaktadır.7 Ölüm Ağı, hava, kara, deniz, uzay ve siber alanlardaki tüm sensör ve etki unsurlarının merkeziyetçi olmayan, esnek ve kendi kendini iyileştirebilen bir ağ yapısında birleşmesidir.7 YZ ajan ağı sayesinde, bir dronun kamerası düşmanı tespit ettiğinde bu bilgi üst karargaha gönderilmez; dronun içindeki ajan, hemen çevredeki topçu birliklerinin, savaş uçaklarının veya siber taarruz unsurlarının YZ ajanlarıyla yatay olarak iletişim kurar.7 Hangi unsurun mühimmatı var, hangisi daha iyi açıda, hangisinin vurulma riski daha düşük gibi parametreler makine hızında hesaplanır ve hedef tahsisi saniyeler içinde yapılır.7 Bu ağ yapısında bir düğüm (örneğin bir radar) yok edilse bile, RL algoritmaları rotaları saniyesinde yeniden optimize ederek alternatif düğümleri devreye sokar ve ağın işlevselliğini sürdürür.7

2. Akademik Teoriler Yapay zekâ destekli askeri tahmin sistemlerinin kavramsal olarak inşa edilebilmesi için çok güçlü matematiksel temellere ve algoritmik teorilere ihtiyaç vardır. Bu teorilerin odağında karar teorileri, pekiştirmeli öğrenme varyasyonları, Markov süreçleri ve oyun teorisi yer almaktadır.

Sistemlerin belirsizlik altında, eksik bilgiyle ve son derece dinamik, hasmane bir ortamda çalışabilmesi, bu akademik temellerin doğrudan harp sahasına uyarlanmasıyla mümkündür.

2.1. Markov Karar Süreçleri ve Belirsizlik Altında Karar Alma

Harp sahasının asimetrik doğası ve "savaşın sisi" (fog of war) olarak adlandırılan belirsizlik ortamı, akademik literatürde "Kısmi Gözlemlenebilir Markov Karar Süreçleri" (Partially Observable Markov Decision Processes - POMDP) ile modellenmektedir.14 Askeri bir karar alıcı veya otonom bir sistem, hiçbir zaman düşmanın tam konumunu, moral durumunu, cephane miktarını veya niyetini yüzde yüz kesinlikle bilemez. Sensörlerden gelen veriler gürültülü olabilir, düşman elektronik aldatma (spoofing) yapıyor olabilir. POMDP, eylemlerin optimum dizisini planlarken mevcut eksik bilgiyi Bayesçi ağlar (Bayesian networks) gibi olasılıksal yöntemlerle günceller ve yönetir.15 Matematiksel bir modelleme yapıldığında, çok etmenli bir operasyon ortamı (örneğin düşman hava savunmasına karşı bir otonom İHA sürüsü saldırısı) Merkeziyetçi Olmayan Kısmi Gözlemlenebilir Markov Karar Süreci (Dec-POMDP) olarak formüle edilir.14 Bu formülasyon şu

parametreleri içerir:

● (Ajan Kümesi): Savaş alanında karar alan, koordine olan dost unsurlar (İHA'lar, insansız kara araçları, füzeler).

● (Durum Uzayı): Savaş alanının anlık durumu (Düşman mevzileri, topografya, hava durumu). Ajanlar bu durumu tam olarak bilemezler.

● (Eylem Uzayı): Ajanların gerçekleştirebileceği manevralar (Radar frekansını değiştirme, tırmanma, ateş etme, sessizliğe bürünme).

● (Geçiş Olasılığı): Seçilen bir taktiğin çevreyi veya düşmanı nasıl etkileyeceğinin olasılıksal dağılımı.

● (Ödül Fonksiyonu): Operasyonun başarı kriteri. Düşman unsurunu asgari sivil zayiatla ve asgari dost unsur kaybıyla yok etmek en yüksek pozitif ödülü getirirken, hedefi ıskalamak veya dost ateşi (blue-on-blue) negatif ödül (ceza) getirir.

● ve (Gözlemler ve Gözlem Olasılıkları): Sensörlerden elde edilen parazitli verilerin veya eksik istihbaratın olasılıkları.

● (İskonto Faktörü): Gelecekte elde edilecek stratejik bir kazanımın, anlık taktiksel kazanıma göre ne kadar önemseneceğini belirleyen zaman faktörü.

Bu denklemin çözülmesi, özellikle telsiz sessizliğinin (EMCON) uygulandığı veya iletişimin koptuğu senaryolarda ajanların önceden öğrendikleri politikalara dayanarak otonom işbirliği yapmasını sağlar.17

2.2. Çoklu Etmenli Pekiştirmeli Öğrenme (Multi-Agent Reinforcement Learning - MARL)

Eğer muharebe alanında tek bir merkezi süper bilgisayar her şeyi yönetseydi, bu bir tek nokta hatası (single point of failure) yaratırdı. Modern teori, dağıtık ajanların ortak (kooperatif) veya rekabetçi hedefler doğrultusunda eğitildiği Çoklu Etmenli Pekiştirmeli Öğrenme (MARL) yaklaşımlarına dayanmaktadır.17 Çeşitli simülasyon ortamlarında ajanlar, çevreyle milyonlarca kez

etkileşime girerek eylem-durum çiftlerini öğrenir ve ödül fonksiyonunu maksimize etmeye çalışırlar.

Ajanların savaş alanının tamamını göremediği durumları aşmak için Derin Tekrarlayan Q-Ağları (Deep Recurrent Q-Network - DRQN) ve PPO (Proximal Policy Optimization) gibi mimariler kullanılır.17 MARL sistemlerinde karşılaşılan en büyük akademik açmaz "kredi ataması" (credit assignment) sorunudur. Düşman birliğinin başarıyla pusuya düşürüldüğü bir senaryoda, bu başarının hangi İHA'nın radarı, hangi kara aracının manevrası veya hangi elektronik harp unsurunun karıştırması sayesinde gerçekleştiğini algoritmik olarak belirlemek zordur. Sistemi optimize etmek için ödülün doğru eyleme atanması gerekir ve bu, güncel akademik araştırmaların en yoğunlaştığı alanlardan biridir.17

2.3. Hiyerarşik Pekiştirmeli Öğrenme (Hierarchical Reinforcement Learning - HRL)

Orduların askeri harekat planlaması, sonsuz ufuklara sahip (long-horizon) ve seyrek ödüller (sparse rewards) barındıran muazzam karmaşıklıkta bir eylem uzayı sunar. Satranç veya Go oyununda olduğu gibi her hamlenin anlık bir tepkisi yoktur; askeri bir hamlenin sonucu günler sonra ortaya çıkabilir. Bu karmaşıklığı yönetmek için akademi, görevi zamansal ve mekansal olarak soyut alt politikalara bölen Hiyerarşik Pekiştirmeli Öğrenme (HRL) algoritmalarına yönelmiştir.22 Askeri komuta kontrol yapısını ve

hiyerarşisini birebir taklit eden bu algoritmada karar mekanizması, bir "Genel Komutan" (makro/stratejik seviye) ve "Operasyon Komutanları"

(mikro/taktiksel seviye) olmak üzere hiyerarşik katmanlara ayrılır.22 Akıllı Komutan (Smart Commander) çerçeveleri altında, üst düzey YZ ajanı ana operasyonel hedefleri (örneğin, "X tepesini ele geçir") belirler. Bu yüksek seviyeli hedef, alt seviyedeki uzmanlaşmış ajanlara iletilir.

Alt düzey ajanlar (örneğin zırhlı birlik rotalama ajanı, mühimmat lojistik ajanı, hava desteği ajanı) bu büyük görevi kendi dar kapsamlarında nasıl optimize edeceklerine karar verirler.20 Bu hiyerarşik ayrım, eylem uzayının karmaşıklığını drastik biçimde azaltır ve gerçekçi operasyonel senaryolarda sistemin ölçeklenebilir bir hızda öğrenmesine olanak tanır.22

2.4. Oyun Teorisi, Öz-Oyun (Self-Play) ve Nash Dengesi

Pekiştirmeli öğrenmenin muharebe taktikleri geliştirmesindeki en büyük gücü Oyun Teorisi ve Öz-Oyun (Self-play) mekanizmalarından gelir.24 Ajan, önceden programlanmış insan taktiklerini taklit etmek yerine, kendi kopyalarına veya algoritmik varyasyonlarına karşı milyonlarca kez savaşır. Bu sıfır toplamlı asimetrik simülasyonlarda ajan, rakibin en ufak zafiyetini sömürmek ve kendi savunmasını güçlendirmek için sürekli evrim geçirir.

Eğitim süreci oyun teorisindeki Minimax prensiplerine ve Nash dengesi arayışına dayanır.24

Sistem, rakibin en iyi karşı hamlesine karşı kendi kaybını minimize edecek stratejiyi seçer. Bunun sonucunda YZ, insan mantığına ters gelebilen (counter-intuitive), son derece agresif veya görünüşte mantıksız ancak matematiksel ve fiziksel olarak en kusursuz muharebe manevralarını keşfeder.27 İkili uçak it dalaşı (dogfight) senaryolarında kullanılan Soft Actor-Critic (SAC) algoritmaları ile entegre edilen rekabetçi öz-oyun eğitimleri, uzman insan bilgisini tamamen dışlayarak sıfırdan ölümcül hava muharebesi stratejileri yaratabilmektedir.24

3. Sistem Mimarisi YZ destekli tahmine dayalı askeri sistemlerin sahada uygulanabilmesi için salt algoritmik kodlardan çok daha fazlasına ihtiyaç vardır. Sistem mimarisi; donanım, veri altyapısı, ağ topolojisi, iletişim protokolleri ve algoritmik güvenlik katmanlarından oluşan sofistike bir

bütündür. Bu sistemler, kırılgan olan merkezi savaş karargahlarından ziyade uca (edge computing) kaydırılan işlemler etrafında şekillenmektedir.

3.1. Nöro-Sembolik YZ Mimarisi (Neuro-Symbolic AI) ve Etik Uyum

Sadece Derin Pekiştirmeli Öğrenme (DRL) ve nöral ağlara dayanan otonom silah sistemleri (LAWS), operasyonel komutanlar ve uluslararası hukuk açısından devasa riskler barındırır.28 Nöral ağlar (Deep Learning), verileri hızla analiz edip karmaşık desenleri bulmada olağanüstü başarılı olsalar da, çalışma prensipleri bir "kara kutu" (black box) niteliğindedir.27 Eğer otonom bir İHA sivil bir hedefi vurursa veya bir dost ateşine (blue-on-blue) sebep olursa, komutanlar veya denetimciler sistemin o spesifik kararı neden aldığını (nöral ağırlıkların nasıl şekillendiğini) açıklayamazlar.27 Askeri harekatın Silahlı Çatışma Hukukuna (LOAC), Angajman Kurallarına (ROE) ve Cenevre Sözleşmelerine uygun olması yasal bir zorunluluktur ve kara kutu sistemleri bu hukuki zemini sarsar.28 Bu yaşamsal sorunu çözmek için savunma sanayii, "Nöro-Sembolik YZ" mimarilerine geçiş yapmaktadır. Bu mimari, veri güdümlü nöral ağların adaptif öğrenme kapasitesini, kural tabanlı sembolik mantığın yorumlanabilir, şeffaf ve deterministik doğası ile hibritler.28

Mimari Katman İşlevi ve Yetenekleri Askeri Uygulama Örneği

Nöral Katman (Derin Büyük veriyi işleme, Uydu görüntülerindeki Öğrenme) kalıp/desen tanıma, çevre kamuflajlı tankları tespit algısı, istatistiksel tahmin. etme, düşman radar sinyallerini sınıflandırma.

Sembolik Katman Açık kuralları uygulama, "Eğer hedef hastane sınırları (Mantıksal Çıkarım) mantıksal kısıtlamalar içindeyse, ateşleme getirme, yorumlanabilirlik, mekanizmasını kilitle" yasalara uyum. kuralını sert kodlamak.

Entegre Nöro-Sembolik Dinamik durumlara adapte DARPA ANSR ve RAID Ajan olurken belirlenmiş sınırların programlarında geliştirilen dışına çıkmamayı garanti güvenilir taktiksel ajanlar. eden güvenilir otonomi.

Bu mimaride sembolik katman, nöral ağın ihlal edemeyeceği kesin mantıksal çitler (fences) oluşturur. Böylece YZ sistemi yaratıcı taktikler

geliştirirken, insani değerleri ve hukuku asimile ederek etik sınırları aşmaz.28

3.2. JADC2, ABMS ve TITAN: Donanım ve Bulut Entegrasyon Altyapısı

Makine hızında karar almanın omurgasını, devasa sensör ağlarını birleştiren teknolojik altyapılar oluşturur. ABD Savunma Bakanlığı'nın JADC2 (Joint All-Domain Command and Control) konsepti, dünyanın farklı yerlerindeki sensörleri ve vurucu unsurları tek bir ağ üzerinde birleştirmeyi hedefler.32 Bu yapının Hava Kuvvetleri ayağını ABMS (Advanced Battle Management System) oluşturur.

ABMS, geleneksel ayrık platformların aksine sensörler, veri füzyonu, yapay zekâ destekli karar motorları ve bulut tabanlı işlem gücünden oluşan canlı bir ekosistemdir.32 Kara Kuvvetleri ayağında ise TITAN (Tactical Intelligence Targeting Access Node) programı öne çıkar. TITAN, uzaydaki uydulardan, yüksek irtifa hava araçlarından ve yerdeki radarlardan gelen terabaytlarca ham veriyi makine öğrenmesi modelleriyle sentezleyerek sensörden vurucuya (sensor-to-shooter) geçen zamanı eşine rastlanmamış biçimde kısaltır.33

3.3. CTDE: Merkezi Eğitim, Merkeziyetçi Olmayan İcra

Çok etmenli otonom sistemlerde iletişim bant genişliği son derece değerlidir ve düşman tarafından sürekli karıştırılmaya (jamming) maruz kalır. CTDE (Centralized Training and Decentralized Execution) mimarisi bu soruna çözüm sunar.17 Mimari, yaşam döngüsünü ikiye ayırır:

1. Merkezi Eğitim (Centralized Training): Ajanlar (örneğin otonom İHA sürüleri), güvenli üslerde veya devasa simülasyon sunucularında toplanan global veriler kullanılarak merkezi olarak eğitilir. Bu aşamada her ajan diğerlerinin konumunu, stratejisini ve elde ettiği ödülleri görebilir.

2. Merkeziyetçi Olmayan İcra (Decentralized Execution): Savaş alanına (gerçek dünyaya) konuşlandırılan ajanlar, sahip oldukları algoritmik ağırlıklarla tamamen bağımsız hareket ederler. İletişim kopsa, ana karargah vurulsa bile ajanlar görevlerini koordine bir şekilde yerine getirmeye devam eder, çünkü simülasyon evresinde iletişim olmadan nasıl işbirliği yapacaklarını öğrenmişlerdir.18

4. Gerçek Dünya Vakaları

Akademik makalelerdeki matematiksel formüllerin ve konseptlerin teoride kalmadığını, doğrudan harp sahasına entegre edildiğini kanıtlayan dönüm noktası niteliğinde gerçek dünya vakaları mevcuttur.

4.1. **DARPA ACE Programı**, AlphaDogfight ve X-62A VISTA Yapay zekânın askeri havacılıktaki evriminde en kritik kilometre taşı DARPA'nın "Air Combat Evolution" (ACE) programıdır.26 2019 ve 2020 yıllarında sanal ortamda gerçekleştirilen "AlphaDogfight Trials", hava muharebesinin geleceğini şekillendirmiştir. Bu denemelerde Heron Systems (daha sonra Shield AI çatısı altına girmiştir) tarafından geliştirilen ve derin pekiştirmeli öğrenme teknikleriyle (hiçbir insan girdisi olmadan, tamamen öz-oyun ile) eğitilen YZ ajanı, deneyimli bir insan F-16 pilotunu 5-0 gibi net bir skorla mağlup etmiştir.26 Simülasyonlar gerçek zamandan çok daha hızlı çalıştırılarak, YZ'nin on binlerce yıllık uçuş tecrübesini birkaç ayda kazanması sağlanmıştır. Sistem, insan pilotların hayatta kalamayacağı riskleri alarak veya reflekslerinin yetmeyeceği reaksiyon sürelerinde (milisaniyeler) kararlar üreterek eşi görülmemiş taktikler sergilemiştir.

Bu sanal başarının ardından en büyük meydan okuma "simülasyondan gerçeğe" (sim2real) geçiş olmuştur. Simülasyonda aerodinamik sürtünmeler, hava durumu ve sensör gürültüsü her zaman kusursuz yansıtılamaz. ACE ekibi ve Shield AI, geliştirdikleri algoritmaları X-62A VISTA (Variable In-flight Simulator Test Aircraft) isimli modifiye edilmiş, açık sistem mimarisine sahip bir F-16 platformuna entegre etmiştir.26 2022'de, ABD Hava Kuvvetleri ve MIT YZ Hızlandırıcı ekibi (DAF AIA) tarafından geliştirilen "Sıvı Zaman Sabitli Nöral Ağlar" (Liquid Time-constant Networks) isimli yepyeni bir algoritma sınıfı sayesinde aylar süren eğitim süreci haftalara indirilmiştir.37 X-62A VISTA, insanlı bir F-16'ya karşı yüksek G kuvvetleri altında gerçek savaş manevralarını tamamen otonom icra ederek havacılık tarihinde devrim yaratmıştır.26 ABD Hava Kuvvetleri Sekreteri Kendall, sistemi bizzat havada izleyerek yapay zekânın ölümcül muharebe senaryolarındaki güvenilirliğini tescillemiştir.36

4.2. DARPA Deep Green: Geleceği Hesaplayan Komuta Sistemi

İnsan komutanların savaşın devasa bilgi yükü altında ezilmesi probleminden yola çıkan DARPA, komutanı destekleyen **"Deep Green"** (Derin Yeşil) sistemini geliştirmiştir.8 IBM'in satranç ustası Garry Kasparov'u yenen Deep Blue sisteminden ilham alan isim, sistemi makineye devretmekten ziyade komutan güdümlü (commander-driven) bir teknoloji yaratmayı amaçlamıştır.11 Deep Green, savaş alanında sensörlerden gelen gerçek zamanlı durumu (execution monitoring) sürekli izler. Ardından, sahadaki dost ve düşman birliklerinin olası etkileşimlerini simüle eden hızlı RL döngüleri çalıştırır. Sistem, "eğer düşman sağ kanattan saldırırsa", "eğer hava desteği gecikirse" gibi yüzlerce çatallanan olasılığı önceden hesaplayarak alternatif planlar üretir.8 Bu yetenek, bir komutanın operasyon kontrolden çıkmaya başladığında "ne yapacağım" demek yerine, Deep Green'in çoktan hazırlamış olduğu optimize edilmiş seçenekler arasından "hangisini seçeceğim" aşamasına geçmesini sağlar. Böylece ordular potansiyel düşmanlarından daha hızlı ve çeyrek personelle düşünme/planlama yeteneğine kavuşur.10

4.3. Harp Oyunları (Wargaming) ve AFSIM Entegrasyonu

ABD Hava Kuvvetleri, geleceğin silah sistemlerini ve taktiklerini test etmek için AFSIM (Advanced Framework for Simulation, Integration, and Modeling) adlı C++ tabanlı çok alanlı modelleme ve simülasyon çerçevesini kullanmaktadır.6 AFSIM, yüzlerce sanal sensörün, uçağın ve silahın gerçek fizik kurallarına göre birbirleriyle etkileşime girdiği devasa bir kum havuzudur (sandbox).39 RAND Corporation raporlarına göre, pekiştirmeli öğrenme araçlarının (AFSIM Reinforcement Learning Tool) doğrudan bu sisteme entegre edilmesi stratejik çalışmalara yön vermektedir.6 İnsanların oynadığı harp oyunları dijitalleştirilmekte (discourse and decisionmaking datası toplanmakta), bu veriler üzerinden yapay zekâ, insanların taktiksel sınırlarını aşan asimetrik senaryolar üretmektedir.41 C++ tabanlı yapısı ve TensorFlowLite destekleri sayesinde Python darboğazları aşılarak modelin inanılmaz hızlarda milyonlarca simülasyon iterasyonu yapması sağlanmaktadır.41

4.4. 2025-2026 Ufku: İsrail-İran "Hiper-Savaş" Vakası

Açık kaynak istihbarat ve konsept raporlarına göre 2025-2026 dönemi, YZ entegreli savaşların "hiper-savaş" (hyperwar) aşamasına ulaştığını kanıtlamaktadır. İncelenen İsrail-İran "12 Gün Savaşı" gibi spesifik senaryolarda/vakalarada, İsrail'in hava savunma ve YZ-C2 mimarileri, uydulardan inen veriyi, yüzlerce İHA beslemesini, sinyal istihbaratını (SIGINT), düşman füzelerinin telemetri kayıtlarını ve siber alanlardaki hareketliliği gerçek zamanlı operasyonel ağlarda birleştirmiştir.42 Yüzlerce balistik füze ve insansız hava aracının aynı anda ateşlendiği doyum noktası (saturation) saldırılarında, insan operatörlerin hedefleri ayırması ve savunma silahlarını tahsis etmesi fiziksel olarak imkansızdır. Bu vakalar, savunma sistemlerinin büyük ölçüde otonom algoritmaların inisiyatifine ve makine hızındaki karar mekanizmalarına devredilmesinin bir zorunluluk olduğunu göstermektedir.42

5. Mekanizma Analizi Makine hızında karar alma sistemlerinin, özellikle RL ve YZ Ajan Ağlarının muharebe sahasında çalışmasını sağlayan mekanizmalar, muazzam teknolojik yeteneklerin yanı sıra aşılması zor kronik problemler de barındırmaktadır.

5.1. C-UAS (Karşı İnsansız Hava Aracı) Savunmasında Otonom Koordinasyon

Modern harp sahasını domine eden ucuz ve sürü halinde hareket eden dronlara (UAV) karşı eski nesil "Bul, Sabitle, Bitir" (Find-Fix-Finish) mekanizmaları hantal kalmaktadır. Mevcut sistemler, dağınık ve çevik hedeflere karşı "Tespit Et, Karar Ver, Yok Et" (Detect-Decide-Defeat) adı verilen otonom ölüm zincirlerine dönüşmektedir.43 Mekanizma şu şekilde çalışır: Sürü halindeki düşman dronları tespit edildiğinde, YZ Ajanı problemi bir "Kısmi Gözlemlenebilir Markov Karar Süreci" (POMDP) olarak formüle eder.16

Sistemin içindeki yüksek seviyeli bilişsel ajanlar (RL ajanları), hangi düşman dronunun dost kritik altyapıya daha yakın olduğunu, taşıdığı tahmini patlayıcı yükünü ve rotasını saniyenin onda biri sürede analiz ederek bir "önceliklendirme" yapar.16 Ardından, hedeflerin özelliklerine göre (elektronik karıştırmaya açık mı yoksa kinetik bir mermiyle mi düşürülmeli) angajman tipi seçilir.

Bu mekanizma, komuta kontrol sistemlerindeki yüksek seviyeli bilişsel fonksiyonlar (hedefi seçme) ile düşük seviyeli harekete geçirici fonksiyonların (silahı ateşleme) birbirinden mükemmel biçimde ayrıştırılmasını sağlar.16

5.2. Spektrum Tahsisi ve Çevresel Optimizasyon

Elektronik harp ortamında radyo frekanslarının ve iletişimin sürdürülebilmesi kritik bir unsurdur.

Dağıtık Dinamik Spektrum Erişimi (DSA) mekanizmalarında, çok ajanlı pekiştirmeli öğrenme (MARL) kullanılarak cihazların sınırlı spektrum kaynaklarını bir komut merkezinden emir beklemeden paylaşması sağlanır.17 Aynı şekilde, akıllı yansıtıcı yüzeylerin (RIS/ARIS) bulunduğu bir çevrede operasyon yapan bir askeri drone, sinyal-girişim-gürültü oranı (SINR) kısıtlamaları altında yörüngesini optimize etmek için Derin Deterministik Politika Gradyanı (DDPG) gibi sürekli eylem uzayı algoritmaları kullanır. Drone, düşmanın radar ekolarını ve kendi iletişimindeki parazitleri engellemek için havada doğrusal olmayan manevraları otonom olarak gerçekleştirir.44

5.3. Sistematik Darboğazlar: Veri Ölçeklenmesi, Güven ve Yetenek Açığı

Makine hızında çalışan RL sistemlerinin operasyonel düzeye (geniş kapsamlı C2 uygulamalarına) taşınması önünde devasa engeller raporlanmaktadır.27

1. Astronomik Veri Talepleri: RL ajanları boyutları büyüdükçe katlanarak artan (üstel) oranda eğitim verisine ihtiyaç duyar. Askeri harekatın kapsamı genişledikçe durum uzayı (state space) milyarlarca kombinasyona ulaşır. Savunma Bakanlığının bu devasa algoritmaları eğitecek yüksek kaliteli ve spesifik askeri problem setlerine dayalı veriyi üretme kapasitesi şu an için kısıtlıdır.27

2. Güven Erozyonu (Trust Deficit): Karar süreçlerinin "kara kutu" doğası, hayat-memat meselelerinde sistemin komutanlar tarafından reddedilmesine yol açmaktadır. Büyük askeri harekat süreçleri algoritmik bir çıktı sunduğunda, komutanlar süreci "mantıklı bir süzgeçten" geçiremedikleri için sisteme güvenmemektedirler.27

3. İnsan Kaynağı ve Beyin Göçü: Çok gelişmiş bir algoritma yaratılsa dahi, Savunma Bakanlıkları bu algoritmaları sürdürecek ve kalibre edecek yüksek nitelikli yapay zekâ mühendislerini bünyesinde tutamamaktadır. Özel sektörün son derece rekabetçi ve kazançlı yapısı, orduların nitelikli yetenekleri elinde tutmasına (retention) engel olmakta ve orduyu ticari teknoloji devlerine bağımlı kılmaktadır.3

6. Trend Analizi (2020–2026) Geçtiğimiz 6 yıllık süreçten 2026 ufku ve ötesine bakıldığında, makine hızında karar alma sistemlerinin ulusal orduların envanter yapısını, tedarik süreçlerini ve operasyonel doktrinlerini derinden şekillendirdiği net trendler olarak ortaya çıkmaktadır.

6.1. Otonomi Silahlanma Yarışı ve Kontrolsüz Yayılma (Proliferation)

ABD ve Çin arasındaki Büyük Güç Rekabeti (Great Power Competition), yapay zekâ tabanlı otonom silah sistemlerinin gelişim yörüngesini belirlemektedir. ABD, JADC2 gibi projelerle devasa sensör ağlarını entegre ederek asimetrik bir karar alma avantajı peşindeyken; Çin, "karar-merkezli savaş" (decision-centric warfare) konseptini merkeze alarak yapay zekâ entegrasyonunda başa baş bir teknolojik kapasite inşa etmektedir.47 Ancak en büyük risk, bu teknolojinin iki kutuplu olmaktan çıkmasıdır. Otonom donanımlar, drone bileşenleri ve açık kaynaklı RL algoritmaları (örneğin arXiv'de paylaşılan makaleler ve ticari dronlardaki otopilot yazılımları), orta ölçekli devletlere ve devlet dışı aktörlere hızla yayılmaktadır (proliferation). Bu yayılma, küresel düzeyde tahmin edilemezlik ve dengelemesi çok zor yeni bir güvenlik ikilemi (security dilemma) yaratmaktadır.47

6.2. İnsanlı-İnsansız Sistemlerin Füzyonu: Seçmeli Pilotlu Platformlar

DARPA ACE ve X-62A VISTA'nın başarılarının ardından, tam otonom savaş platformlarının gökleri domine edeceği bir döneme girilmektedir. ABD Hava Kuvvetleri, F-35 gibi dünyanın en gelişmiş

5. nesil savaş uçaklarını "Seçmeli Pilotlu" (Optionally Piloted) hale getirecek programlara hız vermiştir.48 2026'nın sonlarında F-35'in yarı otonom veya tam otonom uçuş kabiliyetlerinin ilk gösterimlerinin yapılması, 2027'de ise operasyonel testlere başlanması hedeflenmektedir. Bu trendin

temel motivasyonu; gelişmiş A2/AD (Geçişe Kapatılmış/Alan Yasaklama) ortamlarında, düşmanın yoğun hava savunma ağları içinde bir insan pilotun hayatta kalma şansının düşük olmasıdır. Uçağı riske atmadan, makine hızında manevralar yapabilen YZ'nin kontrolü devralması, hava kuvvetlerinin derin darbe yeteneklerini garanti altına almaktadır.48

6.3. LLM (Büyük Dil Modelleri) ve RL (Pekiştirmeli Öğrenme) Hibrit C2 Ağları

2024 ve 2026 arasında YZ mimarilerinde gözlemlenen en heyecan verici trend, ChatGPT benzeri Büyük Dil Modelleri (LLMs) ile Pekiştirmeli Öğrenmenin birleştirilmesidir.21 Bir komuta kontrol senaryosunda, komutanın askeri jargon kullanarak doğal dille verdiği "Bölgedeki iletişim hatlarını kes ve düşmanı baskıla" şeklindeki genel stratejik emir, LLM tarafından algılanıp yüksek seviyeli bir planlama matrisine dönüştürülmektedir. Ardından, bu makro strateji, arka planda çalışan binlerce RL ajanına mikro görevler (hedef tespiti, radar açısı, uçuş yörüngesi) olarak aktarılır.7 Bu mimari, insan komutan ile makine (Centaur model) arasındaki arayüz problemini çözerken, strateji ile taktiksel uygulamanın arasındaki gecikmeyi tamamen ortadan kaldırmaktadır.

7. Stratejik Sonuçlar Makine hızında karar alan pekiştirmeli öğrenme modellerinin ulusal güvenlik cihazlarına entegrasyonu, siyaset bilimi, uluslararası ilişkiler, caydırıcılık teorisi ve harp tarihi açısından derin stratejik sonuçlar doğurmaktadır.

7.1. Algoritmik İstikrar ve Krizlerin Tırmanması (Escalation Dynamics)

Yapay zekâ sistemleri devasa bir hız sağlarken, devlet adamlarının uluslararası krizleri yönetme zamanını ellerinden almaktadır. Geçmişteki **"Küba Füze Krizi"** gibi diplomasinin ve sağduyunun günlerce zaman kazandırdığı krizlerin, saniyeler içinde karar alan algoritmalarla yönetilmesi durumunda tırmanma (escalation) kontrolden çıkabilir.2 Devletler kriz anlarında rakip devleti diplomatik olarak ikna etmeye çalışırken, sahadaki YZ modelleri karşı tarafın bir radar sinyalini veya otonom dronunun sınırı birkaç metre geçmesini anında "varoluşsal bir saldırı hazırlığı" olarak yorumlayıp, makine hızında önleyici vuruş (pre-emptive strike) kararı alabilir.

Caydırıcılık (Deterrence) artık sadece nükleer füzelerin sayılarıyla değil, bu sistemleri yöneten "kod satırlarının" kararlılığıyla ölçülmektedir.2 Hasım devletlerin birbirlerinin algoritmalarının nasıl çalıştığını bilememesi (istihbarat boşluğu), nükleer eşiğin altındaki bölgesel çatışmalarda devletleri yanlış hesaplamalara iterek istenmeyen "Kaza Savaşlarına" (Flash Wars) sürükleme potansiyeli taşımaktadır.2

7.2. "Sentor" Doktrininin Kaçınılmazlığı: İnsan Etik ve Stratejik Zırhı

Otomasyon teknolojisinin cazibesine rağmen YZ, duygudan, korkudan, siyasi sezgiden ve uluslararası etiğin getirdiği bağlamdan bütünüyle yoksundur. ABD Kongresi önündeki uzman ifadelerinde belirtildiği üzere, YZ uluslararası rekabetin karakterini dönüştürse de, güç kullanımının ve insan iradesinin çarpışmasının doğasını (nature of war) değiştiremez.2

Stratejik mükemmeliyet, insanı devreden çıkarmak değil, "Sentor Savaşı" (Centaur Warfighting) modelinde insan ve makineyi birleştirmektir.4 Makinenin eşsiz hız ve hesaplama yeteneği, komutanın ahlaki sorumluluğu, siyasi öngörüsü ve yaratıcılığı ile tamamlanmalıdır.

Nöro-Sembolik YZ mimarilerinin LOAC (Silahlı Çatışma Hukuku) uyumluluğu ile de pekiştirilen bu gereklilik 28, insanın tetiği çeken "son onayı" veren (human-in-the-loop) merci olmasının hukuki ve stratejik bir zorunluluk olduğunu teyit eder.

7.3. Rekabet Asimetrisi ve Bürokratik Çeviklik

Geleceğin güç dengesi; kimin en akıllı YZ algoritmasını yazdığından ziyade, bu algoritmaları eğitecek "veri altyapısına", hesaplama kapasitesine (compute) ve bürokratik çevikliğe kimin sahip olduğuyla belirlenecektir. ABD Senatosu İstihbarat Komitesi oturumlarında altı çizildiği gibi; uygun veri altyapısı kuramayan, eski usul silo tipi komuta kontrol (C2) mimarilerinde ısrar eden ordular için "21. yüzyılda YZ desteği olmayan bir general, bar kavgasında gözleri bağlı bir adam" konumuna düşecektir.3 Makine hızındaki algoritmik savaş konsepti artık teorik bir senaryo veya laboratuvar aşamasındaki bir araştırma değil; doğrudan sahadaki varoluşsal bir gerçektir. Orduların, makine hızında düşünme yeteneğine karşı yavaş karargah süreçleriyle hayatta kalması imkansızdır.

Geleceğin ulusal güvenlik mimarisi; pekiştirmeli öğrenme modellerine milyonlarca farklı ölümü simüle ettirebilen, JADC2 gibi ağlarla sensörleri ve füzeleri birbirine bağlayan ve en önemlisi YZ-Ajan Ağının (AI Agent Mesh) amansız hızı ile insanın ahlaki-stratejik fren mekanizmasını kusursuz biçimde entegre edebilen güçlerin tekelinde olacaktır.

Alıntılanan çalışmalar

1. Decision Making in the Age of the Machine (part 1), erişim tarihi Haziran 3, 2026, https://nllp.jallc.nato.int/iks/sharing%20public/20260320_u_white %20paper_decisi on%20making%20in%20the%20age%20of%20the %20machine.pdf

2. Algorithmic Stability: How AI Could Shape the Future of Deterrence, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-de terrence

3. Addressing the National Security Implications of AI - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/addressing-national-security-implications-ai

4. Mission-Oriented Research for AI and Big Data for Military Decision Making, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/document/mission-oriented-research-for-ai-and-big-da ta-for-military-decision-making-2/

5. Mission-Oriented Research for AI and Big Data for Military Decision Making Executive Summary - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-T R-IST-173/$TR-IST-173-ES.pdf

6. Understanding the Limits of Artificial Intelligence for Warfighters - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA1722-1.html

7. AI-Centric Command and Control – Novum Bellum, erişim tarihi Haziran 3, 2026, https://novumbellum.org/en/ai-centric-command-and-control/

8. Artificial Intelligence for Decision Support in Command and Control Systems - FOI, erişim tarihi Haziran 3, 2026,

https://foi.se/download/18.41db20b3168815026e010/1548412090368/Artificial-int elligence-decision_FOI-S--5904--SE.pdf

9. (PDF) The Deep Green concept - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/220954349_The_Deep_Green_concept

10.Programming Coup D'Oeil: The Impact of Decision Making Technology in Operational Warfare - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/tr/pdf/ADA525275.pdf

11. Deep Green: Commander's tool for COA's Concept - International Institute of Informatics and Systemics (IIIS), erişim tarihi Haziran 3, 2026, https://www.iiis.org/cds2008/cd2008sci/CCCT2008/PapersPdf/T520JF.pdf

12.Kill Web Archives - Ronin's Grips, erişim tarihi Haziran 3, 2026, https://blog.roninsgrips.com/tag/kill-web/

13.Exploring Decision Advantages - Improving Speed, Precision and Efficiency in Military Targeting by Applying Artificial Intelligence - Diva-portal.org, erişim tarihi Haziran 3, 2026, https://www.diva-portal.org/smash/get/diva2:1952579/FULLTEXT01.pdf

14.Multi-Agent Reinforcement Learning Considering Agent Priority for Weapon–Target Assignment | Journal of Aerospace Information Systems, erişim tarihi Haziran 3, 2026, https://arc.aiaa.org/doi/10.2514/1.I011676

15.Artificial Intelligence-Enabled Military Decision-Making Process - Marine Corps University, erişim tarihi Haziran 3, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/J AMS-vol-16-no-2/Artificial-Intelligence-Enabled-Military-Decision-Making-Proce ss/

16.Reinforcement Learning for Decision-Level Interception Prioritization in Drone Swarm Defense - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2508.00641v2

17.Cooperative Multi-Agent Reinforcement Learning Based Distributed Dynamic Spectrum Access in Cognitive Radio Networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2106.09274

18.[2106.09274] Cooperative Multi-Agent Reinforcement Learning Based Distributed Dynamic Spectrum Access in Cognitive Radio Networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2106.09274

19.A Reinforcement Learning Approach to Military Simulations in Command: Modern Operations - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel7/6287639/10380310/10540085.pdf

20.Scaling Reinforcement Learning through Feudal Multi-Agent Hierarchy - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1201723.pdf

21.Harnessing Language for Coordination: A Framework and Benchmark for LLM-Driven Multi-Agent Control - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2412.11761v1

22.Smart Commander: A Hierarchical Reinforcement Learning Framework for Fleet-Level PHM Decision Optimization - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.07171v1

23.advancing military decision support: reinforcement learning-driven - Proceedings of the 2025 Winter Simulation Conference E. Azar, A. Djanatliev, A. Harper, C.

Kogler, V. Ramamohan, A. Anagnostou,, erişim tarihi Haziran 3, 2026, https://www.informs-sim.org/wsc25papers/con154.pdf

24.Hierarchical reinforcement learning from competitive self-play for dual-aircraft formation air combat | Journal of Computational Design and Engineering | Oxford Academic, erişim tarihi Haziran 3, 2026, https://academic.oup.com/jcde/article/10/2/830/7069331

25.Adversarial Attacks on Reinforcement Learning Agents for Command and Control - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2405.01693v1

26.Autonomous Drones Will Not Replace Fighter Pilots, They Will Be Their Wingmen - Belfer Center, erişim tarihi Haziran 3, 2026, https://www.belfercenter.org/sites/default/files/2025-06/AutonomousDrones%2C %20Moscioni%2C%20DETS.pdf

27.Risk Assessment of Reinforcement Learning AI Systems: Looking..., erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA1473-1.html

28.Neuro-Symbolic AI for Military Applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2408.09224

29.Neuro-Symbolic AI for Military Applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2408.09224

30.Neuro-Symbolic AI for Military Applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2408.09224v2

31.Neuro-Symbolic AI for Military Applications - Semantic Scholar, erişim tarihi Haziran 3, 2026, https://www.semanticscholar.org/paper/Neuro-Symbolic-AI-for-Military-Applicati ons-Hagos-Rawat/9083fb4b4662627067628c1f3aa526fdaaeb0172

32.Advanced Battle Management System: Needs, Progress, Challenges, and Opportunities Facing the Department of the Air Force (2022), erişim tarihi Haziran 3, 2026, https://www.nationalacademies.org/read/26525/chapter/3

33.Reducing the Risks of Artificial Intelligence for Military Decision Advantage - CSET, erişim tarihi Haziran 3, 2026, https://cset.georgetown.edu/wp-content/uploads/CSET-Reducing-the-Risks-of-A rtificial-Intelligence-for-Military-Decision-Advantage.pdf

34.Priority-Aware Multi-Agent Deep Reinforcement Learning for Resource Scheduling in C-V2X Mode 4 Communication - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/6287639/6514899/11072434.pdf

35.Op-ed: Would You Let an AI Be Your Wingman? - Fung Institute for Engineering Leadership, erişim tarihi Haziran 3, 2026, https://funginstitute.berkeley.edu/news/85887/

36.Autonomy for the World: X-62 VISTA - Shield AI, erişim tarihi Haziran 3, 2026, https://shield.ai/autonomy-for-the-world-x-62-vista/

37.Training Environment for High Performance Aircraft Reinforcement Learning - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2505.01953

38.Training Environment for High Performance Aircraft Reinforcement Learning - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.01953v1

39.Understanding the Limits of Artificial Intelligence for Warfighters: Volume 5, Mission Planning - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1700/RRA172 2-5/RAND_RRA1722-5.pdf

40.Multi-Agent Mission Planning with Reinforcement Learning - CEUR-WS.org, erişim tarihi Haziran 3, 2026, https://ceur-ws.org/Vol-2819/session1paper1.pdf

41.Understanding the Limits of Artificial Intelligence for Warfighters: Volume 1, Summary - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1700/RRA172 2-1/RAND_RRA1722-1.pdf

42.AI technologies in recent wars and armed conflicts (2010–2026), erişim tarihi Haziran 3, 2026, https://arvak.am/en/ai-technologies-in-recent-wars-and-armed-conflicts-2010-2 026/

43.The New Front Lines: How CUAS is Redefining Superiority in an Invisible Battlespace - Blog, erişim tarihi Haziran 3, 2026, https://blog.squadra.vc/articles/the-new-front-lines-how-cuas-is-redefining-sup eriority-in-an-invisible-battlespace

44.Enhancing Battlefield Awareness: An Aerial RIS-assisted ISAC System with Deep Reinforcement Learning - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2405.20168v1

45.[2301.00124] Situation-Aware Deep Reinforcement Learning for Autonomous Nonlinear Mobility Control in Cyber-Physical Loitering Munition Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2301.00124

46.Observer-Based Deep Reinforcement Learning for Robust Missile Guidance and Control, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/document/10887184/

47.(PDF) AUTONOMOUS WEAPONS SYSTEMS IN GREAT POWER COMPETITION: A COMPARATIVE ANALYSIS OF UNITED STATES AND CHINA DEVELOPMENT TRAJECTORIES, 2020-2026 - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/403017949_AUTONOMOUS_WEAPON S_SYSTEMS_IN_GREAT_POWER_COMPETITION_A_COMPARATIVE_ANALYSIS_OF_ UNITED_STATES_AND_CHINA_DEVELOPMENT_TRAJECTORIES_2020-2026

48.Optionally Piloted F-35 Set to Redefine Air Combat: Lockheed Unveils 2025 Vision, erişim tarihi Haziran 3, 2026, https://thedefensewatch.com/aerospace-aviation/why-the-u-s-optionally-piloted -f-35-could-redefine-fighter-jet-combat/

49.Scalable Interactive Machine Learning for Future Command and Control - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2402.06501

Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken yapay zekâ destekli tahmin yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası model güvenilirliği, makine hızı, insan denetimi ve stratejik bağlam üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir. Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi

okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar. Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle yapay zekâ destekli tahmin alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?
  - Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi?

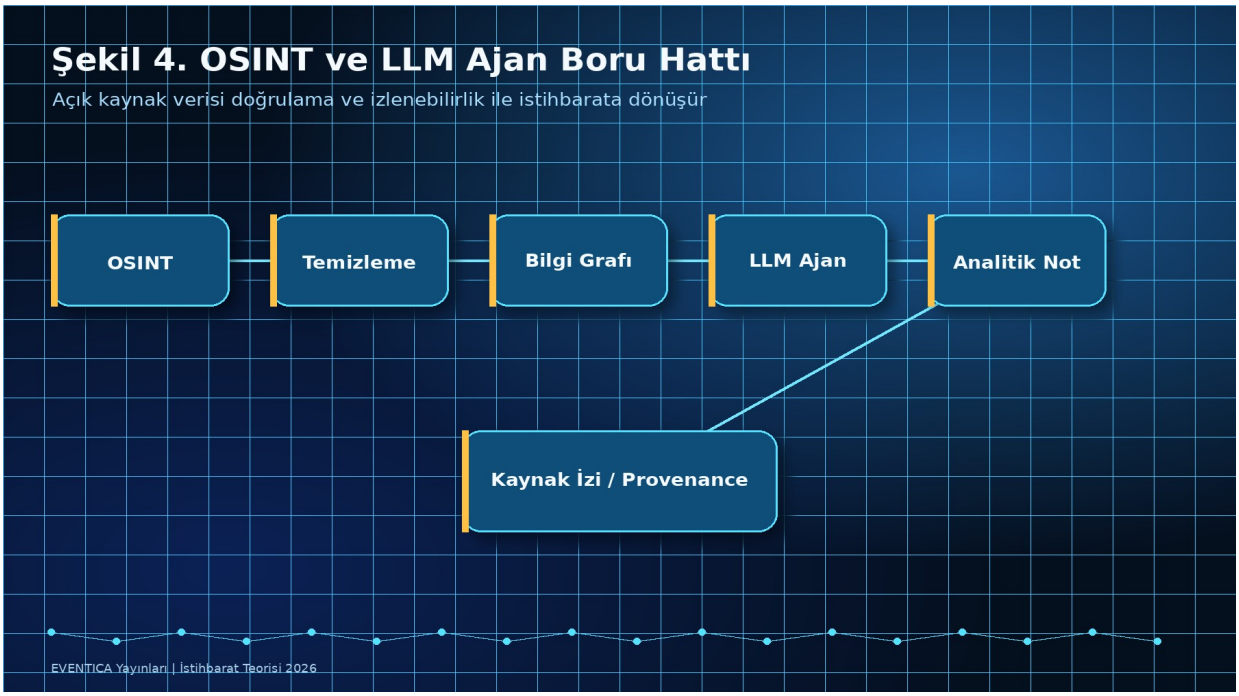
- Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?
- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı?
- Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?
- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı?
- Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Yapay Zekâ Destekli Tahmin Sistemleri ve Makine Hızında Karar Alma alanında en güçlü erken uyarı göstergeleri hangileridir?
2. Bu göstergeler hangi durumda yanlış pozitif üretir?
3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?
4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma sağlanmalıdır?
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı anlamlara gelir?
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?
8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 4. OSINT, Veri Mühendisliği Boru Hatları ve LLM Ajanları

OSINT'in değeri ham veri bolluğunda değil; temizlenmiş, kaynaklandırılmış, bağlama oturtulmuş ve karar ürününe dönüştürülmüş veri hattındadır.



Şekil 5. OSINT verisinin karar ürününe dönüşme hattı

Tablo 7. OSINT boru hattı kalite kontrolleri

Aşama	Kontrol	Çıktı
Toplama	Hukuki erişim ve kaynak kaydı	İzlenebilir ham veri
Temizleme	Tekrar, gürültü ve eski gösterge temizliği	Kullanılabilir veri seti
Zenginleştirme	Bağlam, zaman, coğrafya ve aktör eşleştirme	Analitik veri
Modelleme	Özellik ve hipotez testi	Önceliklendirilmiş sinyal
Ürünleme	Güven seviyesi ve karar eşiği	İstihbarat ürünü

Bölüm 4: OSINT ve Veri Mühendisliği Boru Hatları: Pasif Keşif, Özellik Mühendisliği ve Büyük Dil Modellerinin Otonom Terminal Yetenekleri

Kavramsal Çerçeve Modern stratejik istihbarat ve siber güvenlik mimarisi, bilgi toplama süreçlerinden otonom yürütme aşamalarına kadar uzanan köklü bir paradigma değişimi yaşamaktadır. Bu dönüşümün merkezinde, Açık Kaynak İstihbaratı (OSINT), veri mühendisliği boru hatları (data engineering pipelines) ve Büyük Dil Modelleri (LLM) tabanlı otonom ajanların eşi görülmemiş entegrasyonu yer almaktadır. Geleneksel istihbarat döngüsünde OSINT, çoğunlukla yapılandırılmamış verilerin manuel olarak incelenmesi, tasnif edilmesi ve insan analistler tarafından anlamlandırılması süreçlerine dayanmaktaydı.1 NATO'nun stratejik tanımlamalarına göre istihbarat, bilginin yönlendirilmiş toplanması ve işlenmesi sonucunda ortaya çıkan bir üründür ve bu süreçte iletişimsel stratejiler ile fiziksel eylemler arasındaki uyum kritik bir rol oynar.2 Ancak artan veri hacmi ve siber tehdit enflasyonu, bu verilerin algoritmik olarak işlenmesini, özellik mühendisliği (feature engineering) ile yapılandırılmasını ve nihayetinde otonom terminal yeteneklerine sahip yapay zekâ ajanları tarafından doğrudan aksiyona dönüştürülmesini mutlak bir zorunluluk haline getirmiştir.1 ABD Ulusal İstihbarat Direktörlüğü'nün (ODNI) yayımladığı "IC OSINT Stratejisi 2024-2026" raporu, istihbarat topluluğunun artık basit bir kamu görevlileri hiyerarşisi olmaktan çıktığını; bunun yerine ajanslar, yükleniciler, satıcılar, platformlar, danışmanlar, veri brokerları, siber güvenlik firmaları, bulut sağlayıcıları, yapay zekâ sistemleri, yabancı ortaklar ve giderek artan bir şekilde açık kaynak katmanında faaliyet gösteren sivil unsurlardan oluşan devasa bir "montaj"

(assemblage) haline geldiğini açıkça ortaya koymaktadır.4 Modern istihbarat, sivil hizmet boru hatlarını aşan teknik kapasiteler, dilsel uzmanlık, siber uzmanlık, veri mühendisliği ve devasa analitik ölçek gerektirmektedir.5 Bu karmaşık ekosistem içinde pasif keşif (passive reconnaissance), bir hedefin sistemlerine doğrudan müdahale etmeden veya hedefi uyarmadan, kamuya açık ağlardan, DNS kayıtlarından, sosyal medyadan ve sızdırılmış veri tabanlarından bilgi toplama süreci olarak tanımlanır.7 Pasif keşif, siber operasyonların ve istihbarat faaliyetlerinin temelini oluşturur. Hedef ağın topolojisi, kullanılan teknolojiler ve potansiyel

güvenlik açıkları bu aşamada, port taraması (örneğin Nmap) gibi hedefi uyaran aktif tarama yöntemlerine başvurulmadan haritalandırılır.7 Geleneksel yaklaşımlarda pasif keşif verileri oldukça gürültülü ve düzensizdir. Yapılandırılmamış serbest OSINT verilerinin doğrudan Güvenlik Operasyon Merkezlerine (SOC) veya Tehdit İstihbarat Platformlarına (TIP) aktarılması, "sinyal-gürültü oranının" katastrofik seviyelere düşmesine ve analist yorgunluğuna yol açmaktadır.1 Tipik bir güvenlik operasyon merkezi, açık kaynaklı tehdit akışlarını sisteme entegre ettikten sadece günler sonra binlerce geçersiz uyarı (false positive), eski gösterge (stale indicator) ve yinelenen veri ile boğuşmakta; sonuç olarak analistler bu verileri incelemeyi tamamen bırakmaktadır.1 Bu durum, açık kaynak istihbaratının işe yaramaz olduğu yanılgısını doğursa da, asıl problemin "ücretsiz veri" değil, "yapılandırılmamış veri" olduğu veri mühendisliği disiplini tarafından kanıtlanmıştır.1 Bu darboğazı aşmak için veri mühendisliği boru hatları devreye girmektedir. Özellik mühendisliği, toplanan ham OSINT verilerinden model eğitimi ve tehdit tespiti için en anlamlı, öngörülebilir sinyallerin (özniteliklerin) matematiksel ve istatistiksel yöntemlerle çıkarılması işlemidir.10 DNS çözümleme kalıpları, sertifika otoritesi ilişkileri, ağ topolojisi karakteristikleri ve dilsel öznitelikler, veri mühendisliği süreçlerinden geçerek makine öğrenmesi modellerinin tüketebileceği heterojen veri setlerine dönüştürülür.10 Bu süreç, deneylerden üretim aşamasına geçişte veri bilimcilerinin sıklıkla karşılaştığı "Jupyter Notebook İkilemi"ni (Notebook Dilemma) aşarak, modellerin operasyonel hale getirilmesini (operationalizing) ve üretim kalitesinde (production-ready) veri boru hatlarının oluşturulmasını sağlar.14

Kavramsal çerçevenin son, en yenilikçi ve en yıkıcı katmanını ise Büyük Dil Modellerinin (LLM) otonom terminal yetenekleri oluşturmaktadır. Özellik mühendisliği ile rafine edilen ve makine öğrenmesi modelleri tarafından skorlanan istihbarat, artık sadece insan analistlere sunulan bir rapor olmaktan çıkmış; karar verme yetisine sahip, hafızalı, bağlamı anlayabilen ve mantıksal yürütme (reasoning) döngülerini kullanabilen otonom ajanlara aktarılmaya başlanmıştır.15 LLM ajanları, salt birer metin üreticisi (NLG) olmaktan çıkarak, izole edilmiş korumalı alanlarda (sandbox) komut satırı arayüzlerini (CLI) kullanabilen, bash komutları yazabilen, ağ taramaları

yapabilen ve pasif keşif verilerini kullanarak aktif sömürü (exploitation) senaryolarını otonom olarak yürütebilen dijital operatörlere dönüşmüştür.17 "İnternet Protokolünden Kabuk Erişimine"

(IP-to-Shell) kadar olan bu süreç, insan müdahalesi olmadan tamamlanabilmekte ve siber güvenlikte otonomi çağını başlatmaktadır.17 Bu üçlü entegrasyon (OSINT, Veri Mühendisliği, Otonom Ajanlar), devlet ve devlet dışı aktörler arasındaki istihbarat kapasitesi uçurumunu daraltırken, taktiksel sahada karar alma süreçlerini milisaniyeler seviyesine indiren algoritmik savaşın yapıtaşlarını inşa etmektedir.21 Bu durum, uluslararası ilişkilerde, askeri stratejilerde ve kurumsal güvenlik mimarilerinde riskin ve fırsatın aynı anda asimptotik olarak artmasına neden olmaktadır.

Akademik Teoriler OSINT veri boru hatlarının inşası, verilerin makine öğrenmesiyle analiz edilmesi ve LLM ajanlarının terminal düzeyinde otonom karar alabilmesi; bilgi teorisi, istatistiksel öğrenme, bilişsel ajan mimarileri ve modern savaş teorileri üzerine kurulu derin akademik temellerle desteklenmektedir.

Bilgi Teorisi ve Shannon Entropisi Modellemesi

Özellik mühendisliğinin en temel akademik dayanaklarından biri, ağ üzerindeki anormal yapıları tespit etmek için kullanılan Bilgi Teorisidir (Information Theory). Özellikle, Alan Adı Üretme Algoritmaları (DGA - Domain Generation Algorithm) ile siber suçlular tarafından otonom olarak oluşturulan binlerce kötü amaçlı alan adının tespiti, alan adındaki karakter dizilimlerinin bilgi entropisine dayanır.10 İnsanlar tarafından anımsanması kolay olması için tasarlanan meşru alan adları düşük entropiye sahipken, algoritmik olarak rastgele üretilmiş kötü niyetli alan adları yüksek entropiye sahiptir. Akademik literatürde, bir alan adının rastgelelik derecesi Shannon Entropisi formülü ile modellenir.11 Algoritma, alan adını Derinlik Öncelikli Arama (Depth-First Search - DFS) yöntemi kullanılarak çok dilli bir sözlük seti üzerinden kelimelere böler. En düşük toplam entropiye sahip kombinasyon, alan adının en iyi sözlük temsili olarak seçilir. Kelime entropisi şu denklem üzerinden işler 11:

Burada, sözlükteki uzunluğundaki kelimelerin sayısının toplam kelime sayısına oranını temsil eder. Shannon entropisi, kelimelerin dilsel

özelliklerinden sapmaları ölçerek yüksek bilgi entropisine sahip anlamsız dizilimleri deterministik olarak siber tehdit sinyalleri (özellikleri) şeklinde sınıflandırır.11 Bu yaklaşım, pasif DNS analizi gibi OSINT faaliyetlerinde ham, incelenmesi imkansız verilerin sayısallaştırılarak bir makine öğrenmesi özellik vektörüne dönüştürülmesini sağlar.

İstatistiksel Öğrenme: Gelişmiş Gradyan Arttırma ve Özel Kayıp Fonksiyonları

Makine öğrenmesi teorisinde, heterojen OSINT verilerini sınıflandırmak ve risk skorlaması yapmak için karar ağaçlarının birleştirilmiş (ensemble) formları kullanılır. Akademik çalışmalar, Nöral Ağların (Neural Networks) siber güvenlikte kullanılmasına yönelik erken dönem çabaların, OSINT özelliklerinin yüksek derecede karışık (metin, sayısal, kategorik) doğası nedeniyle yakınsama (convergence) sorunlarıyla karşılaştığını göstermiştir.10 Benzer şekilde, Rastgele Orman (Random Forest) algoritmaları da gradyan arttırmanın sunduğu ardışık iyileştirme (sequential refinement) yeteneklerinden yoksun oldukları için spesifik risk değerlendirmelerinde yetersiz kalmıştır.10 Bu sorunları çözmek için güncel akademik çerçeveler, Gradyan Arttırılmış Karar Ağaçları (GBDT) mimarisine, özellikle de Chen ve Guestrin'in XGBoost (eXtreme Gradient Boosting) uygulamasına dayanmaktadır.10 Ancak siber güvenlik risk değerlendirmesi için temel XGBoost algoritması yeterli değildir; algoritma, güvenliğe özgü özel kayıp fonksiyonlarını (security-specific loss functions) içerecek şekilde ağır modifikasyonlardan geçirilir. Objektif fonksiyon matematiksel olarak şu şekilde formüle edilir:

Objektif fonksiyon matematiksel olarak şu şekilde formüle edilir:

$$\mathbf{Obj = \Sigma_i\, l(y_i, \hat{y}_i) + \Sigma_k\, \Omega(f_k)}$$

Bu denklemde $l(y_i, \hat{y}_i)$ kayıp fonksiyonudur. Bu fonksiyon, hedefin gerçek siber tehdit etiketi y_i ile modelin tahmini $\hat{y}_i$ arasındaki farkı, yani hatalı sınıflandırmanın maliyetini ölçer. $\Omega(f_k)$ terimi ise sisteme eklenen her bir karar ağacının karmaşıklığını cezalandıran ve aşırı öğrenmeyi, yani overfitting riskini azaltan düzenlileştirme bileşenidir.

XGBoost mimarisinde düzenlileştirme terimi genellikle şu şekilde ifade edilir:

$$\Omega(f) = \gamma T + 1/2\ \lambda \|w\|^2$$

Burada T, karar ağacındaki yaprak sayısını; w, yaprak ağırlıklarını; γ, yeni yaprak eklemenin maliyetini; λ ise model karmaşıklığını sınırlayan düzenlileştirme katsayısını temsil eder. Bu yapı sayesinde model yalnızca eğitim verisine ezberci biçimde uyum sağlamaz; aynı zamanda daha genellenebilir, daha dengeli ve risk değerlendirmelerinde daha güvenilir sonuçlar üretir.

Siber güvenlik ve OSINT tabanlı risk skorlama bağlamında bu yaklaşım özellikle önemlidir. Çünkü hatalı negatifler, yani gerçek bir tehdidin düşük riskli görülmesi, çoğu zaman hatalı pozitiflerden daha yüksek operasyonel maliyet üretir. Bu nedenle güvenlik odaklı modellerde kayıp fonksiyonu yalnızca genel doğruluğu değil; tehdidin ciddiyetini, yanlış sınıflandırmanın etkisini ve karar sürecinde oluşturacağı riski de dikkate alacak şekilde tasarlanmalıdır.

arasındaki farkı, yani hatalı sınıflandırmanın maliyetini ölçer.10 terimi ise sisteme eklenen her bir karar ağacının karmaşıklığını cezalandıran ve aşırı öğrenmeyi (overfitting) engelleyen düzenlileştirme (regularization) parametresidir.10 Bu adaptasyon, karmaşık OSINT özelliklerinin yüksek boyutlu uzayda en düşük hata payıyla sınıflandırılmasını garanti eder.

Yoğunluk Tabanlı Kümeleme ve Karşılıklı Güçlendirme Mimarisi

İstatistiksel gözetimli öğrenmenin (supervised learning) sınırlarını aşmak ve önceden tanımlanmamış davranışsal anomalileri, sıfırıncı gün zafiyetlerini (zero-day) veya yapılandırılmamış OSINT sızıntılarındaki aykırı kalıpları tespit etmek için DBSCAN (Gürültülü Uygulamaların Yoğunluk Tabanlı Mekansal Kümelemesi) algoritması teoriye entegre edilmiştir.10 DBSCAN, veri noktalarının vektör uzayındaki yoğunluğuna bakarak herhangi bir kümeye dahil edilemeyen aykırı değerleri (outliers) keşfeder. Sistem, GBDT (risk skorlaması) ve DBSCAN (anomali tespiti) algoritmaları arasında çift yönlü bir geri bildirim döngüsü uygular. Bu mekanizma, akademik dilde "Karşılıklı Güçlendirme Mimarisi" (Mutual Reinforcement Architecture) olarak tanımlanır ve sınıflandırma ile kümeleme sonuçlarının birbirini sürekli olarak

doğrulamasını sağlayarak toplam doğruluk oranını teorik üst sınırlara yaklaştırır.10 ReAct (Akıl Yürütme ve Eyleme Geçme) Paradigması

LLM'lerin gerçek dünyada terminal komutlarını otonom olarak yürütebilmesi, siber güvenlik araştırmalarında yaygın olarak benimsenen "ReAct" (Reasoning and Acting) bilişsel çerçevesine dayanır.20 ReAct teorisi, yapay zekânın karmaşık operasyonel görevleri (örneğin port taraması, zafiyet testi, aktif sömürü) ardışık bir mantıksal düzlemde yürütmesini sağlar. Sistemin bilişsel mimarisi, süreci bir Sızma Testi Ağacı (Penetration Testing Tree - PTT) olarak modeller.17 Bu ağaç yapısında, her düğüm (node) belirli bir görevi (örn. Nmap taraması) temsil ederken, kenarlar (edges) görevler arasındaki bağımlılıkları ve akıl yürütme akışını tanımlar.17 Bu mimarideki temel bileşenler şunlardır:

1. Re (Task Planning / Akıl Yürütme): Model, sistemdeki mevcut günlükleri (logs), önceki görev çıktılarını ve geçmiş veri tabanındaki "başarı vakalarını" (success cases) inceleyerek bir sonraki adımın ne olması gerektiğine karar verir.17

2. Act (Command Execution / Eylem): Re modülünün stratejisine dayanarak, otonom ajan spesifik, yürütülebilir komut dizileri (bash, python, msfconsole) üretir ve bunları sisteme gönderir.20 Ağaç yapısı, görevler tamamlandıkça, kısmi başarısızlıklar yaşandıkça veya modelin geri izleme (backtracking) yapması gerektiğinde dinamik olarak evrilir.17 Bu döngüsel teori, ajanın hatalardan ders çıkarmasını ve karmaşık siber saldırı vektörlerini insan yönlendirmesi olmaksızın çözmesini olanaklı kılar.

Algoritmik Savaş ve Karar Gecikmesi Teorisi

Makine öğrenmesi ve LLM'lerin savunma ekosistemindeki yeri, sadece yazılım mimarisiyle değil, aynı zamanda askeri doktrinlerle de teorize edilmektedir. NATO Müttefik Dönüşüm Komutanlığı'nın (ACT) benimsediği yeni nesil savaş teorilerinde, "Algoritmik Savaş" konsepti ön plana çıkmaktadır.22 Bu teori, karmaşıklık ve hızın belirlediği modern muharebe ortamında (çok alanlı operasyonlar, sensör ağları, elektronik harp), bilginin işlenmesi ile eyleme geçilmesi arasındaki "karar gecikmesinin" (decision latency) en kritik kırılganlık olduğunu savunur.24 NATO doktrini, yapay zekânın insan yargısını değiştirmek yerine savaş alanını "bağlamak" ve

karar süreçlerini dramatik ölçüde (en az %50) hızlandırmak için bir araç olduğunu varsayar.24 Politik-Askeri Destekli Karar Alma (PM-ADM) teorisi, LLM tabanlı açık kaynak analizinin ve otonom sistemlerin caydırıcılığı korumak için vazgeçilmez bir stratejik avantaj (Decision Advantage) ürettiğini belirtmektedir.25

Sistem Mimarisi Modern siber istihbarat, OSINT analitiği ve otonom operasyon platformları, veri yutma (ingestion) aşamasından başlayıp terminal düzeyinde komut yürütme (execution) aşamasına kadar ilerleyen, çok katmanlı, geri bildirimli ve birbirine entegre üç ana boru hattından (pipeline) oluşan karmaşık bir mimari üzerine inşa edilmiştir.

1. Özellik Mühendisliği ve Veri Boru Hatları (Data Engineering Pipelines)

OSINT veri toplama sürecinde, API'lerden, ticari tehdit istihbaratı akışlarından, sızdırılmış veri tabanlarından ve açık internetten akan veriler ham haldedir. Boru hattının ilk katmanı bu verileri işlenebilir hale getirmekle yükümlüdür.

● Önişleme ve Gelişmiş Tokenizasyon: Özellikle X (Twitter) gibi gayri resmi platformlardan veya hacker forumlarından elde edilen veriler, standart İngilizce sözlük kök bulucuları (lemmatizer) ve siber güvenlik jargonu için özel olarak eğitilmiş tweet/metin tokenizasyon süreçlerinden geçirilir.13 Örneğin, resmi olmayan "Hellooo" gibi kelimeler normalize edilirken, "vulnerability", "linux", "infosec", "wordpress" gibi kritik siber güvenlik terimleri belirlenir.13

● Vektörel Dönüşüm: Normalize edilmiş bu kelime çantaları (bag-of-words), Terim Frekansı - Ters Döküman Frekansı (TF-IDF) modeli uygulanarak matematiksel vektör formlarına dönüştürülür. Bu sayede her bir kelimenin, devasa döküman havuzu içindeki ağırlığı ve önemi hesaplanmış olur.13

● A/B Testi ve Sürüm Kontrolü: Sistemin makine öğrenmesi uygulamalarına aktarılan her bir özellik seti (feature set), veri kaynağı, çıkarım parametreleri ve zamansal kapsam (temporal coverage) gibi bilgileri içeren meta verilerle katı bir şekilde sürümlendirilir.10 Bu mimari, sistem geliştiricilerine ve güvenlik analistlerine özellik algoritmalarında yapılan

değişiklikleri canlı ortamda A/B testine tabi tutma ve yeni özellik seti sorun çıkardığında eski sürüme sorunsuz geri dönme (rollback) imkanı sunar.10

● Özellik Sürüklenmesi (Feature Drift) İzleme: Siber tehdit manzarası sürekli evrim geçirdiği için, çıkarılan özelliklerin istatistiksel dağılımı zamanla geçerliliğini yitirir (drift).

Boru hattına entegre edilen özellik sürüklenmesi izleme algoritmaları, özelliklerin istatistiksel özelliklerini sürekli izler ve dağılımda modelin doğruluk oranını düşürecek belirgin bir sapma gözlemlendiğinde makine öğrenmesi modelinin yeniden eğitilmesi (retraining) gerektiğini merkeze raporlar.10

2. Otonom Ajan Koordinasyon ve Bilişsel Mantık Katmanı Makine öğrenmesi modelleri tarafından rafine edilen ve risk skorlaması yapılan veri, çoklu ajan (multi-agent) mimarisine dayanan bir koordinasyon katmanına beslenir.

● Özelleşmiş Ajan Modülleri (Multi-Agent Architecture): Gelişmiş sistemler, e-posta doğrulama (email verification), günlük analizi (log analysis) ve IP adresi tarama gibi spesifik alanlara adanmış bağımsız ajanlardan oluşur.15 Her bir ajan kendi etki alanında bağımsız olarak çalışır ve verileri "merkezi bağlamsal öneri sistemine" (contextual recommendation system) iletir. Bu merkezi sistem, farklı etki alanlarından (çapraz alan - cross-domain) gelen çıktıları çapraz analiz ederek zaman tabanlı (time-based), çok vektörlü (multi-vector) veya gizli (stealth) saldırı desenlerini yüksek doğrulukla (%93.6 tespit, %97.2 çoklu ajan korelasyonu) tespit eder.15

● Eşik Bekçisi (Gatekeeper) Doğrulaması: Sisteme dışarıdan (örneğin Telegram web kancaları veya API'ler üzerinden) gelen komutlar ve LLM'nin ürettiği yanıtlar doğrudan icraya alınmaz. Merkezi doğrulama ajanı olan "Gatekeeper", komutları denetleyerek sistemde komut/istem enjeksiyonu (prompt/command injection) yapılmasını ve model halüsinasyonlarının kritik sistemlere zarar vermesini engeller.26

● RAG Tabanlı Bellek Yönetimi ve PTT (Sızma Testi Ağacı): Ajanın hafıza yönetimi, görevleri, başarılı/başarısız komut çıkışlarını, hedef IP adresi meta verilerini ve exit_code, exit_class gibi çıkış sonuçlarını düğümlere kaydeden

Sızma Testi Ağacı (PTT) veri yapısı üzerinden koordine edilir.23 Ayrıca, ajanların karar verirken boşluğa düşmesini engellemek için, geçmişteki başarılı sızma testleri ve komut satırı deneyimleri RAG (Retrieval-Augmented Generation) havuzundan çekilerek anlık kararlara rehberlik eder.20 Örneğin RapidPen mimarisi, görev planlaması (Re) için 10 adet özel GPT-4o LLM örneğini (instance), komut üretimi ve log analizi (Act) için ise 8 adet GPT-4o LLM örneğini paralel olarak çalıştırarak devasa bir bilişsel iş gücü yaratır.27

3. İzole Yürütme Ortamları (Code Execution Sandboxes)

LLM'lerin gerçek dünyada bir komut satırı arayüzünü kullanabilmesi için sistem güvenliğini riske atmayan, ancak ajana tam bir bilgisayar ortamı sunan izole yürütme ortamlarına (sandbox) mutlak suretle ihtiyaç vardır. Bu aşama, ajanın dijital operatör kimliği kazandığı noktadır.

Yürütme Ortamı / Mimari Yaklaşım Temel Kullanım Kaynak Araç ve Yetenekleri Durumu / Avantajı

Docker & Ajanın ürettiği Regülasyona tabi Kubernetes kodların geçici sektörler için (OpenSandbox/De (ephemeral) Docker (finans/sağlık) tam erFlow) konteynerlerinde izlenebilirlik, yerinde veya K8s podlarında barındırma çalıştırılıp iş (self-hosted) ve bitiminde yok güvenli tek atımlık edilmesi. Tüm dosya (single-shot) kod işlemleri ve ağ yürütme. istekleri audit logları halinde kaydedilir (OpenTelemetry entegrasyonu).

Modal (gVisor Sunucusuz Güvenilmeyen Tabanlı) (serverless) yapay (untrusted) ajan zeka altyapısı ile kodlarının güvenle gVisor çalıştırılması ve izolasyonunun yoğun hesaplama birleştirilmesi. gerektiren Çalışma zamanında görevlerin (runtime) dinamik eşzamanlı olarak desteklenmesi. tanımlanabilen esnek ortamlar.

İhtiyaç halinde anında GPU ivmelendirmesi sunar.

Blaxel (Perpetual "Sürekli bekleme Uzun oturum süresi Standby) modunda" (session duration) (perpetual standby) gerektiren, optimize kalan 'ajan edilmiş soğuk bilgisayarlar' başlatma (cold mimarisi. Ajan boşta start) performansı kaldığında işlem arayan otonom maliyeti yazmaz, döngüler. ancak saniyeler içinde kaldığı yerden uyanabilir (fast resume).

SWE-World (LLM Ağır Docker Geleneksel ajan Tabanlı Simülatör) konteynerleştirme mimarilerinin altyapı ihtiyacını ortadan darboğazlarını kaldıran, hafif ve (infrastructure LLM destekli bottleneck) aşarak çevresel geri yüksek keşifsel bildirim simülatörü. otonomi sağlamak.

Eylemleri "Navigasyon & Düzenleme" olarak kategorize eder.

Terminus-2 Tamamen otonom, Modellerin terminal İskelesi (Harbor insan girdisi talep ortamındaki bilişsel Framework) etmeyen ve tek bir kapasitelerini araç (interaktif bir değerlendirmek için tmux oturumu) yüksek kullanan iskele performanslı (scaffold) mimarisi. tarafsız bir test LLM tıpkı bir insan yatağı (test bed) gibi tuş vuruşu oluşturmak. gönderir, menülerde ok tuşlarıyla gezinir.

Ek Not: Yerel modelleri çalıştıran ajanların, bulutta barındırılan bir tarayıcı tabanlı terminalde (Browser Terminal Use) işlem yapmasını sağlayan köprü mimarileri de gelişmiştir. Bu yaklaşım, yerel komutların bulut tarafında doğrulanabilir ve denetlenebilir (auditable) bir şekilde çalıştırılmasını sağlayarak kuyruğa alma (queue), zaman aşımı (timeout) ve iptal (cancel) gibi kararlı döngü yönetimleri sunar.33

Gerçek Dünya Vakaları OSINT, özellik mühendisliği ve otonom yapay zekâ ajanlarının kesişimi, salt akademik veya teorik bir konsept olmaktan çoktan çıkmış; hem makro ölçekli jeopolitik stratejilerde, hem NATO seviyesindeki askeri hedefleme süreçlerinde, hem de mikro ölçekli siber güvenlik ihlal vakalarında devrim niteliğinde somut etkiler yaratmıştır.

Vaka 1: Rusya-Ukrayna Savaşı, Kızıldeniz ve OSINT'in Geopolitik Demokratikleşmesi

Uluslararası Stratejik Araştırmalar Merkezi'nin (CSIS) detaylı analizlerine göre, devasa boyutlardaki açık kaynak verilerin ve ticari uydulardan (Maxar, Planet Labs, Capella, BlackSky) gelen ham sensör verilerinin otomatik olarak işlenmesi, tarihte eşi görülmemiş bir istihbarat kapasitesi demokratikleşmesine yol açmıştır.21 Tarihsel olarak elit istihbarat toplama ve analiz kabiliyeti, ABD gibi (FY 2025'te 101.1 milyar dolar bütçeli 18 kurumdan oluşan) devasa kaynaklara sahip devletlerin tekelindeydi.21 Ancak, Rusya'nın Ukrayna'yı işgali sırasında Ukrayna, sınırlı devlet istihbarat altyapısına rağmen, ICEYE (Finlandiya merkezli sentetik açıklıklı radar uydu

şirketi) verilerini sürekli kiralayarak ve bu verileri açık kaynak veri hatlarıyla birleştirerek 7.000'den fazla Rus askeri noktasını otonom sistemlerle haritalandırmış ve yüzlerce varlığı imha etmiştir.21 Ek olarak Ukrayna, HawkEye 360 platformundan sağlanan radyo frekansı (RF) verileriyle GPS karıştırma (jamming) ünitelerini hedeflemiş, sivil OSINT inisiyatifi "Molfar" ise sosyal medya üzerindeki paylaşımları özellik mühendisliğinden geçirerek Rus askerlerinin sahadaki konumlarını milimetrik hassasiyetle ifşa etmiştir.21 Sadece devletler değil, devlet dışı aktörler de bu veri mimarilerinden yararlanmaktadır. İran destekli Husi grupları, gelişmiş bir askeri İstihbarat, Gözetleme ve Keşif (ISR) ağı inşa etmek yerine, abonelik tabanlı genel Otomatik Tanımlama

Sistemi (AIS) verilerini kullanarak Kızıldeniz'deki ticari gemileri yüksek hassasiyetle hedeflemiş ve saldırmıştır.21 CSIS, bu durumu istihbarat kapasitesindeki asimetrik güç dengelerinin değişimi olarak nitelemektedir.

Vaka 2: RapidPen ile Otonom "IP-to-Shell" Siber Sızma

Siber güvenlik alanında LLM ajan mimarilerinin gücünü kanıtlayan en dikkat çekici akademik-operasyonel vaka "RapidPen" platformudur. Daha önceki yarı otonom sistemler, zafiyet taraması sırasında insan analistin onayına (human-in-the-loop) ihtiyaç duyarken, RapidPen tamamen insansız (IP-to-Shell) bir model önermiştir.16 Sisteme sadece bir hedef IP adresi verilir. Başka hiçbir yapılandırma veya zafiyet verisi sağlanmaz. RapidPen ajanı (arka planda çalışan 18 adet GPT-4o örneği), hedefi otonom olarak tarar, pasif keşif verilerini analiz eder, olası zafiyetleri Sızma Testi Ağacında (PTT) planlar, Metasploit Framework'ü (msfconsole) terminal seviyesinde otonom olarak çalıştırır ve hedef sistemi istismar eder.20 Gerçek dünya deneyleri, RapidPen'in vakaların %60'ında sadece 200 ila 400 saniye içinde hedef sistemde başarılı bir ters kabuk (reverse shell) bağlantısı kurarak tam erişim sağladığını kanıtlamıştır.17 Saniyeler süren bu işlem, geleneksel sızma testi ekiplerinin günler süren manuel eforunu ortadan kaldırarak siber sızma maliyetlerini dramatik biçimde düşürmektedir.

Vaka 3: CyberThreat-Eval ve CTI İş Akışlarında İnsan-Makine Sınırları

Yapay zekâ ajanlarının gerçek dünya Açık Kaynak İstihbaratı ve Siber Tehdit İstihbaratı (CTI) üretme yetenekleri, endüstri lideri "CyberThreat-Eval" kıyaslama testleriyle detaylıca analiz edilmiştir.34 Bu platform, LLM ajanlarını standart, çoktan seçmeli sorularla değil; gerçek bir güvenlik analistinin günlük iş akışını yansıtan üç aşamalı (Triyaj, Derin Arama ve TI Taslağı Hazırlama) görevlerle test eder.34 Metrikler, model merkezli (sözcüksel örtüşme) olmaktan ziyade analist merkezlidir; verinin doğruluğu (factual accuracy), içerik kalitesi ve operasyonel maliyeti ölçer.34 Vakalar ve test sonuçları, LLM'lerin karmaşık siber sızıntı detaylarını sınıflandırırken doğru ile yanlış bilgiyi ayırt etmede (halüsinasyon riski) ve nüanslı uzmanlık gerektiren konularda hala bazı zorluklar yaşadığını kanıtlamıştır.34 Bu veriler ışığında, tamamen otonom CTI üretimi yerine, "İnsan-Makine İşbirliği" (Human-Machine Collaboration) olarak bilinen melez bir yapı (XBOW mimarisi gibi) benimsenmiştir.34 LLM'ler saniyeler içinde devasa veriyi tarayıp formatlarken, deterministik kurallar ve insan uzmanlar nihai triyaj ve karar onayını (TRA mekanizması üzerinden sürekli geri bildirimle) üstlenmektedir.26 Vaka 4: NATO'nun Yapay Zekâ Odaklı Yeni Nesil Hedefleme Projesi (NGT) Savunma sanayisi ve askeri ittifak boyutunda, NATO Müttefik Dönüşüm Komutanlığı (ACT), veri boru hatlarını ve algoritmik karar sistemlerini entegre etmek üzere "Yeni Nesil Hedefleme" (Next Generation Targeting - NGT) projesini 2025 Sonbahar Benimseme Kurulu aracılığıyla 2026 yılı için temel işaret (Beacon) projelerinden biri olarak kabul etmiştir.24 Devasa füzeler, dronlar, sensör ağları ve elektronik harp unsurlarından gelen, insan analistlerin tek başına işlemeye yetişemeyeceği hacimdeki veriler, yapay zekâ tarafından işlenmektedir. NGT projesi, mevcut ulusal komuta-kontrol mimarilerini değiştirmeden, ulusal kapasiteleri modüler yapay zekâ, birleştirilmiş (federated) veri akışları ve gelişmiş doktriner temellerle bağlamaktadır.24 Projenin stratejik ve ölçülebilir hedefi, verinin işlenip operasyonel hedefe dönüştürülmesi arasındaki bilgi-karar gecikmesini %50'den fazla azaltarak Müttefik kuvvetlerine eşi görülmemiş bir hız avantajı sağlamaktır.24 NATO bu adımı, 2030 Çok Alanlı Operasyonlar (MDO) vizyonuna ulaşmak ve DIANA (Kuzey Atlantik Savunma

İnovasyonu Hızlandırıcısı) ile akademik ekosistemi askeri entegrasyona dahil etmek için kritik bir sıçrama tahtası olarak kurgulamaktadır.25

Mekanizma Analizi Ajanların salt birer metin okuyucu (pasif gözlemci) olmaktan çıkıp, hedef sistemlere fiziksel komutlar gönderen (aktif yürütücü) varlıklara dönüşmesini sağlayan arka plan sistemleri, oldukça sofistike yazılım-donanım entegrasyonlarına dayanır. Bu geçiş, iç içe geçmiş birkaç temel mekanizma ile açıklanır.

Semantik Pivot (Semantic Pivoting): Pasiften Aktife Geçiş

Gelişmiş LLM ajanlarının, güvenlik zafiyeti ararken kullandığı en kritik mekanizmalardan biri "Semantik Pivot"tur.37 Ajan, ilk aşamada hedef sistemle hiçbir saldırgan etkileşime girmez.

Sistem kullanıcısından tarayıcıda normal bir şekilde gezinmesi istenirken, ajan arka planda sessizce HTTP isteklerini, form verilerini ve API uç noktalarını yakalar (pasif keşif).37 Veri boru hattı, bu yapılandırılmamış trafikten bağlamsal istihbaratı—örneğin sabit kodlanmış kimlik bilgileri (hardcoded credentials), gizli dizin yapıları veya yanıt şemalarını—ayıklar. Semantik pivot mekanizması, ayıkladığı bu stratejik öznitelikleri doğrudan LLM'nin bağlam penceresine (context window) yeniden enjekte eder.38 Model, bu pasif veriden yola çıkarak mantıksal bir sıçrama yapar; otonom olarak mevcut durumu aktif bir sömürü fırsatına bağlar ve zafiyeti sömürmek için gereken özel kodu yazar.

Güven Çerçeveli Geri Alma (Confidence-Aware Retrieval) ve Bağlam Zehirlenmesini Önleme

LLM ajanlarının hedef ağda komut çalıştırırken karşılaştığı en büyük yapısal problemlerden biri "bağlam zehirlenmesidir" (context poisoning).38 Ajan sürekli komut dener, hatalar alır ve bu hataları tekrar okursa, bağlam penceresi gereksiz ve alakasız veriyle dolarak ajanın odağını kaybetmesine, dolayısıyla halüsinasyon görmesine veya kısır döngüye girmesine yol açar.

Modern ajan çerçeveleri (örneğin Automation-Exploit mimarisi), bu sorunu aşmak için "Güven Çerçeveli Geri Alma" mekanizmasını tetikler.38 Eğer saldırı yolu örneğin 10. iterasyonda hala başarılı olamamış ve duraksamışsa (stagnates), sistem RAG üzerinden uzman harici mantıkları (örneğin spesifik bir Metasploit kod parçacığını) anlık saldırı bağlamıyla

anlamsal ilgisine (semantic relevance) göre sıralar ve doğrudan isteme enjekte eder. Bu hedefli enjeksiyon (targeted injection), modelin hafızasını temizleyerek amaca kilitlenmesini sağlar.

Sentetik Veri Üretimi (SDG) ve Doğrulanabilir Ödüllerle Pekiştirmeli Öğrenme (RLVR)

Modellerin daha önce hiç görmedikleri yeni Komut Satırı Arayüzü (CLI) araçlarını güvenle kullanabilmesi için eğitilmesi süreci, ciddi bir veri kıtlığı sorunu yaratır.39 LLM'lerin geleneksel dosyalar yerine yeni bir arayüzü kontrol edebilmesi için NVIDIA gibi kurumlar, Sentetik Veri Üretimi (SDG) ile Doğrulanabilir Ödüllere Dayalı Pekiştirmeli Öğrenmeyi (RLVR - Reinforcement Learning with Verifiable Rewards) birleştiren sistemler geliştirmiştir.39 Grup Göreli Politika Optimizasyonu (GRPO - Group Relative Policy Optimization) ile güçlendirilen bu mekanizmada, model sentetik "tohum" verileri üzerinden CLI araçlarının (örneğin langgraph dev --port 8123) doğru sözdizimini (syntax) öğrenir. Model, çalıştırdığı komutun terminal çıktısını ("Server started successfully on port 8000") okur, başarı durumuna göre algoritmadan doğrulanabilir bir ödül alır ve bu döngü, tek bir GPU'da verimli ve güvenli bir şekilde pekiştirilir.39 Ajan, eylemi gerçekleştirmeden önce (örneğin "Execute langgraph up --wait? [y/N]") insan onayı istemeyi de bu mekanizma aracılığıyla öğrenir.

Yinelemeli Hata Ayıklama Döngüsü ve LLM Yargıç (LLM-as-a-judge)

LLM ajanları, terminal düzeyinde çalışırken aldıkları hatalardan geri dönmek için yinelemeli bir mekanizma kullanır.16 "Terminal-Bench" gibi devasa iskele test platformlarında (74 ile 89 arası terminal görevi içeren) yapılan analizler, ajanların başarısızlıklarının temel nedeninin komut doğrulama veya tutarlılıktan ziyade, kodların işletilmesi (execution errors) sırasında oluşan ortam hataları olduğunu kanıtlamıştır.32 Bir görevde, ajandan stdout (standart çıktı), stderr (standart hata) ve çıkış kodlarını (exit code) yapılandırılmış formatta okunması istenir.40 Ajan, örneğin eksik bir paket hatasını stderr çıktısında okuduğunda, hatayı analiz eder, gerekli paketi yüklemek için terminal komutunu yeniden yazar ve döngüyü yeniden başlatır. Modellerin "erken durma" (early stopping) eğilimine karşı, sisteme "Görevin bittiğinden emin misin? Bu çözümün notlandırılmasına neden

olacak..." şeklinde önleyici istemler (prompting) yerleştirilir.42 Komutların nihai doğruluğunu değerlendirmek için insan açıklayıcıların hızına yetişemeyecek görev ölçeklerinde "LLM-as-a-judge" (Yargıç olarak LLM) mekanizmaları devreye girer.32

Trend Analizi (2020–2026) Geçtiğimiz yedi yıllık süreçte siber istihbarat, makine analitiği ve otomasyon teknolojileri, pasif uyarı platformlarından kognitif otonom ajan mimarilerine doğru radikal bir evrim geçirmiştir.

Dönem Hakim Teknoloji ve Mimari Stratejik Ekosistem Etkisi Yaklaşım ve Trendler

2020 - 2022 Kural Tabanlı SIEM ve Güvenlik Statik OSINT Operasyonlarında Gürültü Krizi: Analistlerin on Ücretsiz veri akışları, imza binlerce hatalı uyarının tabanlı (signature-based) (false positive) altında antivirüs/IDS sistemleri, ezilmesi. Yalnızca bilinen basit SOAR kuralları. (known) zafiyetlere tepki verebilme. Gelişmiş, çok aşamalı APT saldırılarının radarın altından kaçması.1

2023 - 2024 Makine Öğrenmesi (ML) Siber Tehdit Boru Hatları ve AI Enflasyonunun Başlangıcı:

Silahlanması Saldırı maliyetlerinde düşüş.

Devletlerin (NATO, ODNI, GBDT, SVM gibi istatistiksel ABD) ve orduların (Project modeller, özel özellik Maven) yapay zekâyı mühendisliği (TF-IDF, stratejik savunma ve veri Entropi), üretken AI'nin işleme doktrinlerine entegre güvenlik raporlama (CTI) etmeye başlaması.3 testleri.

2025 - 2026 Otonom LLM Ajanları ve İstihbaratın Terminal Entegrasyonu Demokratikleşmesi ve Otonom Taktiksel Hız:

ReAct, Semantik Pivot, Kurumsal ağların otonom Terminal-Bench/Terminus-2 sistemler tarafından gibi iskeleler, RapidPen gibi dakikalar içinde aşılması. insansız "IP-to-Shell" İnsan hızını aşan algoritmik otonom araçları, sürekli hedefleme yetenekleri korumalı alanlar (Blaxel). (NATO NGT). Siber saldırı eşiğinin, sıradan kodlayıcılar için bile neredeyse sıfıra inmesi.17

2026 yılı itibarıyla en bariz trend, siber saldırganlar ve savunmacılar arasındaki asimetrik oyun sahasının şekil değiştirmesidir. LLM tabanlı

ajanların otonom terminal yetenekleri kazanması, sızma testleri, pasif keşif haritalandırması ve OSINT analizi için gereken insan uzmanlık eşiğini neredeyse sıfıra indirmiştir.20 Bir sistem operatörü veya sıradan bir sivil, siber güvenlik uzmanı olmasa bile, yapay zekâ aracılığıyla hedef sistemlere sızabilmektedir.20 Bu durum, akademik literatürde "Siber Tehdit Enflasyonu" (Cyber Threat Inflation) olarak adlandırılmakta olup, siber tehditlerin hacminde, hızında ve hedefe odaklanma kabiliyetinde devasa bir patlama yaratmıştır.3

Ek olarak istihbarat dünyasında insan kaynağı profili de tamamen değişmektedir. Geleneksel casusluğun veya saha istihbaratçılığının yerini veri bilimi almıştır. ABD ve NATO birimleri, "FRIDAY" gibi inisiyatiflerle istihbarat topluluğundaki mevcut personeli veri mühendisliği ve yapay zekâ alanında eğitmekte, astrofizikçileri, veri mühendislerini ve bulut altyapısı uzmanlarını ordunun "hedefleme" ve "istihbarat" kollarının merkezine yerleştirmektedir.44 Trend, bilgi üstünlüğünü (decision advantage) elinde bulunduranın savaşı kazanacağı bir algoritmik çağa işaret etmektedir.25

Stratejik Sonuçlar

Sistem mimarileri, vaka çalışmaları ve algoritmik teorilerin sentezlenmesi, otonom LLM terminal yeteneklerinin askeri, diplomatik, ekonomik ve kurumsal güvenlik paradigmaları üzerinde geri döndürülemez stratejik sonuçlar doğurduğunu açıkça kanıtlamaktadır.

1. Jeopolitik İstihbarat Boşluğunun Kapanması ve Asimetrik Tehditlerin Yükselişi:

Veri mühendisliği ile güçlendirilmiş OSINT altyapıları, küresel bilgi tekeline (soğuk savaş dönemi CORONA uydusu veya gelişmiş casus ağları gibi) sahip devletler ile finansal kaynağı sınırlı devlet dışı aktörler arasındaki uçurumu dramatik bir hızla kapatmaktadır.21 Ticari uydu verilerinin (AIS, RF sinyalleri) ve açık sosyal medya dökümlerinin, maliyetsiz LLM ajanları tarafından işlenerek saniyeler içinde askeri hedefleme raporlarına dönüştürülmesi, operasyon merkezsizleşmesi yaratmaktadır.21 ABD yönetimi, savaş zamanlarında müttefiki olan ticari OSINT sağlayıcıları üzerinde "yönetimli erişim" (managed access) kısıtlamaları ve gecikmeler uygulayarak bilgi akışını kontrol edebilse de, CSIS analizleri bu durumun uzun vadede stratejik bir ticaret dengesizliği (trade-off) yaratacağı

uyarısında bulunmaktadır.21 Sistematik kısıtlamalar, veri alıcılarını alternatif küresel sağlayıcılara iterek Batı'nın veri üzerindeki uzun vadeli nüfuzunu zayıflatma riskini barındırmaktadır.

2. Algoritmik Savaşta Karar Alma Kırılganlıkları ve Kriz Tırmanması (Escalation):

Yapay zekâ sistemlerinin NATO'nun PM-ADM ve NGT (Yeni Nesil Hedefleme) doktrinlerine entegrasyonu, operasyonel hızı katlayarak artırırken, potansiyel güvenlik risklerinin doğasını da değiştirmektedir.24 Atlantic Council ve NATO bilim insanlarının ortak analizlerine göre, ordularda yapay zekânın kullanımı yeni tür bir siber risk (örn. nükleer eşiğin doğrudan düşmesi) yaratmaz; asıl tehlike operasyonların "sonuçlarındaki" yıkıcılıktır.22 Sisteme entegre otonom ajanların karar destek altyapısına yönelik bir veri zehirlenmesi (data poisoning) veya model manipülasyonu, NATO'nun kriz anında veriyi algılama ve aksiyon alma yeteneklerini temelden bozabilir.22

Sistemlerin opaklığı (kara kutu doğası) ve devasa işlem hızları, kriz zamanlarında insan hatasına, yanlış hesaplamaya (miscalculation) ve dolayısıyla konvansiyonel çatışmanın kontrolsüz bir şekilde tırmanmasına (escalation) neden olacak geniş bir hata payı bırakmaktadır.21

3. Küresel Teknoloji Rekabeti, Veri Merkezleri ve Ekonomik Güvenlik:

Siber tehditlerin otonomlaşması ve ajan mimarilerinin yaygınlaşması, "hesaplama gücünü" (compute) ulusal güvenliğin merkezine yerleştirmiştir. CSIS raporları, yapay zekâ rekabetinin ABD-Çin jeopolitik ekseninde sadece bir teknoloji yarışı olmadığını, aynı zamanda bir altyapı ve tedarik zinciri savaşı olduğunu vurgulamaktadır.21 Veri merkezlerinin inşası, bir ülkenin yapay zekâ kapasitesini belirleyen en kritik stratejik altyapı haline gelmiştir.21 Hükümetler, devasa veri merkezlerinin yerel enerji şebekeleri ve temiz enerji hedefleri üzerindeki yükünü, yapay zekâ üstünlüğünün getirdiği ulusal stratejik avantajla dengelemek zorundadır.21 Çin'in (özellikle DeepSeek gibi yükselen modeller üzerinden) küresel bir inovasyon merkezi haline gelmesi ve İran gibi müttefikleriyle siber koordinasyonu, Batı blokunu

AI lisanslama (frontier model licensing) ve siber güvenlik çitleri (guardrails) oluşturmaya zorlamaktadır.21

4. Gizlilik Efsanesinin Çöküşü ve Otonom Savunma Direncinin Zorunluluğu:

Ajan destekli pasif keşif platformlarının vardığı son nokta, kamu veya özel kurumların sahip olduğu dijital ayak izinin tamamen gizlenebileceği inancını yıkmıştır.45 Açık ağlardaki metadatalar, geçmiş DNS kayıtları, üçüncü parti API sızıntıları ve açık port bilgileri, LLM ajanları tarafından (RapidPen gibi platformlarla) bir araya getirilerek herhangi bir kurumun tüm ağ topolojisi ve güvenlik mimarisi dakikalar içinde tersine mühendislikle ortaya çıkarılabilmektedir.20 "Siber tehdit enflasyonu" karşısında, statik kural tabanlı imza tespit sistemlerinin ve yalnızca insana dayalı manuel güvenlik operasyonlarının artık iflas ettiği kanıtlanmıştır.3 Kurumlar ve devletler, asimetrik düşman sistemlerinin hızıyla başa çıkabilmek için savunma altyapılarını aynı şekilde otonom ajanlarla donatmalı, "özellik sürüklenmesini" eşzamanlı izlemeli ve kendi siber altyapılarını, LLM yargıçlarıyla sürekli sızma testlerine (sürekli korumalı alanlar ve güvenli iskeleler üzerinden) tabi tutmalıdır.19 İstihbaratın, keşfin ve hedefin otonomlaştığı bu yeni mimaride, yapay zekânın terminal düzeyinde kullanımı lüks bir kurumsal inovasyon aracı olmaktan çıkmış, varoluşsal bir ulusal ve örgütsel güvenlik doktrini haline gelmiştir.

Alıntılanan çalışmalar

1. From Noise to Intelligence - Engineering an OSINT Pipeline That Works - IBM Community, erişim tarihi Haziran 3, 2026, https://community.ibm.com/community/user/blogs/adithya-turaga/2026/05/18/fro m-noise-to-intelligence-engineering-an-osint-pi

2. Intelligence and Strategic Communication, erişim tarihi Haziran 3, 2026, https://stratcomcoe.org/publications/download/Intelligence-and-StratCom-FINAL.pdf

3. Forewarned is Forearmed: A Survey on Large Language Model-based Agents in Autonomous Cyberattacks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.12786v2

4. A STANDALONE OSINT AGENCY FOR STRONGER NATIONAL SECURITY, erişim tarihi Haziran 3, 2026, https://nationalsecurity.gmu.edu/wp-content/uploads/2025/01/A-Standalone-OSI NT-Agency-for-Stronger-National-Security-FINAL-WEB.pdf

5. Washington's Privateers of Intelligence: From the Culper Ring to the Coming Market for Civilian Spycraft - Bryant McGill, erişim tarihi Haziran 3, 2026, https://bryantmcgill.blogspot.com/2026/04/civilian-spycraft.html?m=1

6. scaling the use of publicly available information across the us government | mitre, erişim tarihi Haziran 3, 2026, https://www.mitre.org/sites/default/files/2025-04/PR-25-1065-Scaling-the-Use-of -Publicly-Available-Information-Across-the-US-Government.pdf

7. Active vs Passive Reconnaissance: 6 Key Differences - CyCognito, erişim tarihi Haziran 3, 2026, https://www.cycognito.com/learn/exposure-management/active-vs-passive-reco nnaissance/

8. What is Cyber Reconnaissance? - SentinelOne, erişim tarihi Haziran 3, 2026, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-cyber -reconnaissance/

9. The Rise and Rise of LLM-powered PenTesting Systems, erişim tarihi Haziran 3, 2026, https://pure.royalholloway.ac.uk/ws/portalfiles/portal/71696115/trarol.pdf

10.Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment, erişim tarihi Haziran 3, 2026, https://www.mdpi.com/2073-431X/14/10/430

11. Ch 5 - Feature Engineering: Science or Art? - Securonix, erişim tarihi Haziran 3, 2026, https://www.securonix.com/blog/ch-5-feature-engineering-science-or-art/

12.AI feature engineering in document prep | Talbot West, erişim tarihi Haziran 3, 2026, https://talbotwest.com/services/data-preprocessing/what-is-feature-engineering

13.D4.2 OSINT data fusion and analysis architecture - European Union, erişim tarihi Haziran 3, 2026,

https://ec.europa.eu/research/participants/documents/downloadPublic?documen tIds=080166e5b8f84b9f&appId=PPGMS

14.Master the Feature Engineering Pipeline: Best Practices and Tips | JFrog ML - Qwak, erişim tarihi Haziran 3, 2026, https://www.qwak.com/post/feature-engineering-pipeline

15.A Multi-Agent System for Cybersecurity Threat Detection and Correlation Using Large Language Models - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/6287639/10820123/11141466.pdf

16.RapidPen: Fully Automated IP-to-Shell Penetration Testing with LLM-based Agents - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2502.16730v2

17.RapidPen: Automated IP-to-Shell Pentesting | PDF | Penetration Test - Scribd, erişim tarihi Haziran 3, 2026, https://www.scribd.com/document/899108949/2502-16730v1

18.Alibaba OpenSandbox: AI Agent Execution Platform - Digital Applied, erişim tarihi Haziran 3, 2026, https://www.digitalapplied.com/blog/alibaba-opensandbox-open-source-ai-agen t-execution

19.How to Give Your AI Agent a Filesystem (Safely): Docker Sandbox + Permission System, erişim tarihi Haziran 3, 2026, https://medium.com/@kacperwlodarczyk/how-to-give-your-ai-agent-a-filesyste m-safely-docker-sandbox-permission-system-74de5dded3f1

20.RapidPen: Fully Automated IP-to-Shell Penetration Testing with LLM-based Agents - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2502.16730v1

21.Responding to OSINT: U.S. Strategy and the Democratization of..., erişim tarihi Haziran 3, 2026, https://www.csis.org/blogs/strategic-technologies-blog/responding-osint-us-stra tegy-and-democratization-intelligence

22.How NATO can integrate AI to prevail in future algorithmic warfare - Atlantic Council, erişim tarihi Haziran 3, 2026, https://www.atlanticcouncil.org/in-depth-research-reports/report/how-nato-can- integrate-ai-to-prevail-in-future-algorithmic-warfare/

23.(PDF) RapidPen: Fully Automated IP-to-Shell Penetration Testing with LLM-based Agents, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/389315145_RapidPen_Fully_Automated _IP-to-Shell_Penetration_Testing_with_LLM-based_Agents

24.Next Generation Targeting Helps NATO Move Faster from Information to Decision, erişim tarihi Haziran 3, 2026, https://www.act.nato.int/article/next-gen-targeting/

25.Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation, erişim tarihi Haziran 3, 2026, https://www.act.nato.int/article/harnessing-artificial-intelligence/

26.AI Automation in Cyber Security. In the modern landscape of offensive… | by Dhiraj Ambigapathi | Medium, erişim tarihi Haziran 3, 2026, https://medium.com/@Darkhue/ai-automation-in-cyber-security-7efa302f0d66

27.RapidPen: Fully Automated IP-to-Shell Penetration Testing with LLM-based Agents - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2502.16730

28.GitHub - bytedance/deer-flow: An open-source long-horizon SuperAgent harness that researches, codes, and creates. With the help of sandboxes, memories, tools, skill, subagents and message gateway, it handles different levels of tasks that could take minutes to hours., erişim tarihi Haziran 3, 2026, https://github.com/bytedance/deer-flow

29.Best Code Execution Sandboxes for AI Agents in 2026 | Modal Blog, erişim tarihi Haziran 3, 2026, https://modal.com/resources/best-code-execution-sandboxes-ai-agents

30.SWE-World: Building Software Engineering Agents in Docker-Free Environments - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2602.03419v1

31.Terminus-2 - Harbor framework, erişim tarihi Haziran 3, 2026, https://www.harborframework.com/docs/agents/terminus-2

32.Terminal-Bench: Benchmarking Agents on Hard, Realistic Tasks in Command Line Interfaces - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2601.11868v1

33.Browser Terminal Use — A Local-to-Cloud Execution Bridge for LLM Agents - Reddit, erişim tarihi Haziran 3, 2026, https://www.reddit.com/r/AI_Agents/comments/1r0473m/browser_terminal_use_a _localtocloud_execution/

34.CyberThreat-Eval: Can Large Language Models Automate Real-World Threat Research?, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2603.09452v1

35.[2603.09452] CyberThreat-Eval: Can Large Language Models Automate Real-World Threat Research? - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2603.09452

36.simon-p-j-r/LLM4Pentest - GitHub, erişim tarihi Haziran 3, 2026, https://github.com/simon-p-j-r/LLM4Pentest

37.Building an AI Harness for LLM Pentesting - Strobes, erişim tarihi Haziran 3, 2026, https://strobes.co/blog/ai-harness-offensive-security-llm-pentest-architecture/

38.A Multi-Agent LLM Framework for Adaptive Offensive Security with Digital Twin-Based Risk-Mitigated Exploitation Preprint Notice - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.22427v1

39.How to Train an AI Agent for Command-Line Tasks with Synthetic Data and Reinforcement Learning | NVIDIA Technical Blog, erişim tarihi Haziran 3, 2026, https://developer.nvidia.com/blog/how-to-train-an-ai-agent-for-command-line-t asks-with-synthetic-data-and-reinforcement-learning/

40.How to Build an Autonomous AI Agent That Executes Terminal Commands, erişim tarihi Haziran 3, 2026, https://dev.to/jigjoy/how-to-build-an-autonomous-ai-agent-that-executes-termi nal-commands-23ke

41.Terminal-Bench 2.0, erişim tarihi Haziran 3, 2026, https://www.tbench.ai/benchmarks/terminal-bench-2

42.Terminal-Bench: Benchmarking Agents on Hard, Realistic Tasks in Command Line Interfaces | OpenReview, erişim tarihi Haziran 3, 2026, https://openreview.net/forum?id=a7Qa4CcHak&referrer=%5Bthe%20profile%20o f%20Di%20Lu%5D(%2Fprofile%3Fid%3D~Di_Lu6)

43.Calibrating NATO's Vision of AI-Enabled Decision Support - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-suppo rt

44.FRIDAY: Unlocking the Power of Open-Source Intelligence for a Data-Driven Army, erişim tarihi Haziran 3, 2026, https://mipb.ikn.army.mil/issues/jul-dec-2025/friday-unlocking-the-power/

45.NATO must recognize the potential of open-source intelligence - Atlantic Council, erişim tarihi Haziran 3, 2026, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-p otential-of-open-source-intelligence/

46.reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities - GitHub, erişim tarihi Haziran 3, 2026, https://github.com/six2dez/reconftw

Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken OSINT ve veri mühendisliği yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası kaynak kökeni, veri temizliği, özellik mühendisliği, LLM ajanları ve ürünleme üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon

riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir. Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar. Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle OSINT ve veri mühendisliği alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

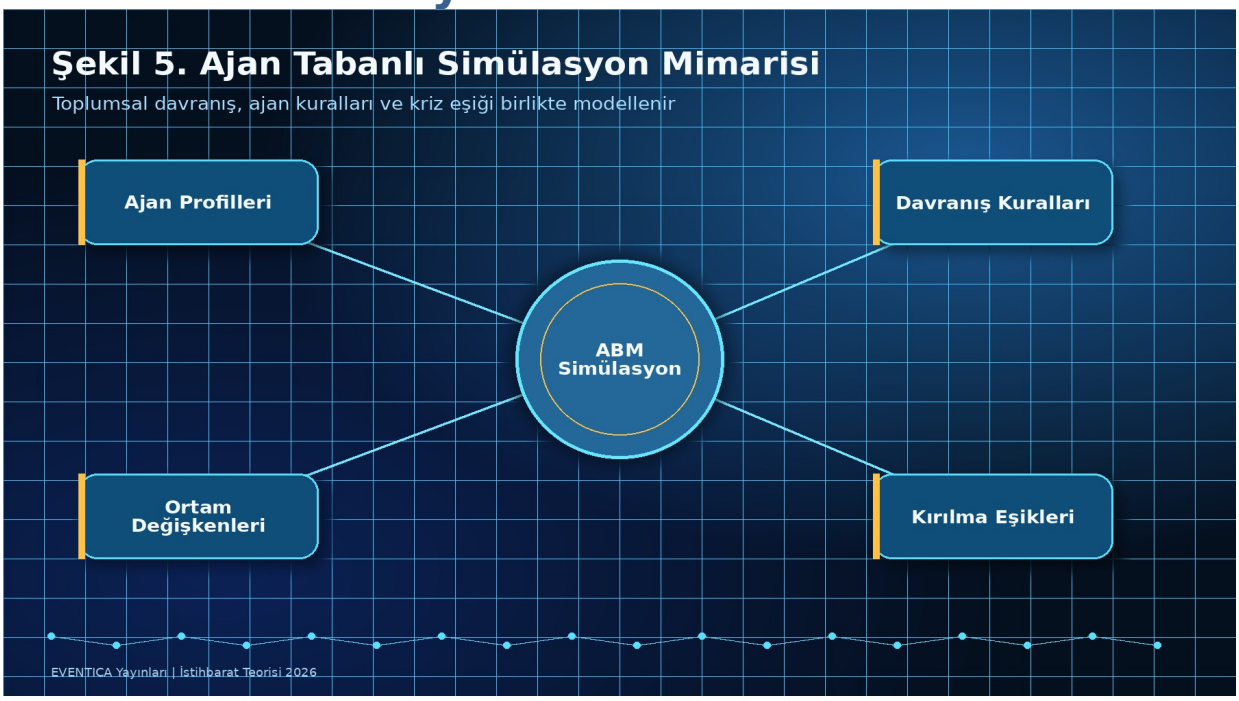
Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?
  - Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi?
  - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?
  - YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı?
  - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?
  - Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı?
  - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. OSINT, Veri Mühendisliği Boru Hatları ve LLM Ajanları alanında en güçlü erken uyarı göstergeleri hangileridir?
2. Bu göstergeler hangi durumda yanlış pozitif üretir?
3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?
4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma sağlanmalıdır?
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı anlamlara gelir?
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?
8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 5. Davranışsal Modelleme ve Ajan Tabanlı Simülasyonlar



Toplumlar tek bir rasyonel aktör gibi davranmaz. Ajan tabanlı modeller, küçük davranış kurallarının büyük sosyal sonuçlara nasıl dönüştüğünü anlamak için kullanılır.

Tablo 8. Ajan tabanlı modelleme kullanım haritası

Kullanım	İstihbarat değeri	Dikkat edilmesi gereken nokta
Kutuplaşma simülasyonu	Toplumsal gerilim eşiklerini görme	Gerçek davranışı birebir temsil etmez
Bilgi yayılımı	Anlatıların hız ve yönünü izleme	Platform etkisi ayrı modellenmelidir
Panik/uyum analizi	Kriz tepkilerini değerlendirme	Psikolojik varsayımlar açık yazılmalıdır
Sentetik ajan testi	Operasyonel senaryoları güvenli ortamda deneme	Model çıktısı karar değil senaryodur

Simülasyonlar

Toplumlar tek bir rasyonel aktör gibi davranmaz. Ajan tabanlı modeller, küçük davranış kurallarının büyük sosyal sonuçlara nasıl dönüştüğünü anlamak için kullanılır.

Tablo 8. Ajan tabanlı modelleme kullanım haritası

Kullanım

İstihbarat değeri Dikkat edilmesi gereken nokta Kutuplaşma simülasyonu Toplumsal gerilim eşiklerini görme Gerçek davranışı birebir temsil etmez Bilgi yayılımı Anlatıların hız ve yönünü izleme Platform etkisi ayrı modellenmelidir Panik/uyum analizi Kriz tepkilerini değerlendirme Psikolojik varsayımlar açık yazılmalıdır Sentetik ajan testi Operasyonel senaryoları güvenli ortamda deneme Model çıktısı karar değil senaryodur Önyargıların Modellenmesi ve Sentetik Etki Ajanları

1. Kavramsal Çerçeve Modern stratejik istihbarat ve güvenlik mimarisi, fiziksel coğrafyaların

ve geleneksel kinetik harp alanlarının ötesine geçerek, insan algısının, inanç sistemlerinin ve karar alma mekanizmalarının doğrudan hedef alındığı davranış merkezli bir çatışma paradigmasına evrilmiştir. Uluslararası güvenlik literatüründe ve askeri doktrinlerde "Bilişsel Harp" (Cognitive Warfare) olarak tanımlanan bu yeni alan, bilginin salt bir iletişim aracı olmaktan çıkıp, hedeflerin gerçekliği algılama biçimlerini algoritmik bir hassasiyetle manipüle eden temel bir silaha dönüştüğü süreci ifade etmektedir.1 Amerika Birleşik Devletleri Savunma Bakanlığı (DoD) ve NATO'nun stratejik değerlendirmeleri, bilişsel harpın geleneksel Psikolojik Operasyonlar (PSYOPS) veya bilgi harbi (information warfare) konseptlerinden radikal biçimde ayrıldığını vurgulamaktadır. Bu yeni doktrinde amaç, kısa vadeli mesajların iletilmesi değil, "insan alanının" (human domain) sürekli ve kesintisiz bir muharebe sahası olarak kabul edilmesi ve hedef kitlelerin tutum, inanç ve rasyonel düşünme kapasitelerinin kalıcı olarak değiştirilmesidir.1 Bu operasyonel dönüşümün teknolojik omurgasını, insan davranışını eşi görülmemiş bir ölçekte ve isabetle haritalandıran Davranışsal Modelleme ve Ajan Tabanlı Simülasyonlar (Agent-Based Modeling - ABM) oluşturmaktadır. Ajan tabanlı modelleme, sistemin bütünsel davranışını ve sonuçlarını yöneten kuralları anlamak amacıyla, otonom veya

yarı otonom ajanların eylemlerini, reaksiyonlarını ve sosyal etkileşimlerini simüle eden hesaplamalı bir yaklaşımdır.3 Geleneksel istatistiksel modellerin aksine ABM, toplumsal olayları yukarıdan aşağıya (top-down) formüllerle dikte etmez; bunun yerine, mikro ölçekteki bireysel ajanların spesifik bilişsel kurallara göre hareket ettiği ve bu sayede makro ölçekte karmaşık sosyal fenomenlerin (kutuplaşma, panik, bilgi yayılımı) kendiliğinden ortaya çıktığı aşağıdan yukarıya (bottom-up) bir belirme (emergence) süreci sunar.3 NATO Baş Bilim İnsanı'nın Bilişsel Harp Raporu, bu sentetik ajanların ve simülasyonların modellenmesinde insan doğasının biyo-psikososyal katmanlarının dikkate alınması gerektiğini ortaya koymaktadır. Bilişsel çatışmaların hedef aldığı manipülasyon seviyeleri üç temel kategoride yapılandırılmıştır 2:

Manipülasyon Seviyesi Operasyonel Odak Taktiksel Hedefler ve Ajan Tabanlı Simülasyon

Çıktıları

Biyolojik Seviye (Kapasite Sinir sistemi ve fizyolojik alt Bireylerin bilişsel Manipülasyonu) yapı kapasitelerini, stres toleranslarını ve karar alma hızlarını doğrudan veya dolaylı uyarıcılarla bozmak, yönlendirmek veya degrade etmek.

Psikolojik Seviye Bilişsel değerlendirme ve Bireylerin duygu (Yorumlama çerçeveleme durumlarını, risk algılarını ve Manipülasyonu) zihinsel şemalarını etkileyerek bilginin yorumlanma biçimini değiştirmek. Ajanların belirli haberlere vereceği histerik veya aparetik tepkilerin simüle edilmesi.

Sosyal Seviye (Uyum Kolektif kimlik ve kurum Sosyal bağları parçalamak, Manipülasyonu) meşruiyeti kimlik politikalarını silahlaştırmak ve epistemik kaos yaratmak.

Simülasyonlarda toplumsal güven ağlarının hangi girdilerle çökeceğinin analiz edilmesi. Bu biyo-psikososyal modelleme, simülasyonların sadece veri işleyen dijital varlıklar değil, aynı zamanda sınırlı rasyonelliğe sahip, yorulabilen, önyargılı ve duygusal tepkiler verebilen "sentetik sosyal varlıklar" olarak tasarlanmasını zorunlu kılmaktadır.2 Geçmişte laboratuvar ortamlarında gerçek insan deneklerle yapılması imkansız veya

etik dışı olan yıkıcı psikolojik testler, artık on binlerce sentetik ajanın bulunduğu kapalı dijital yankı odalarında saniyeler içinde simüle edilebilmekte, böylece uluslararası güvenlik aktörleri için stratejik bir karar avantajı (decision advantage) sağlanmaktadır.1

2. Akademik Teoriler Sentetik etki ajanlarının ve geniş çaplı sosyal simülasyonların

inandırıcılığı, sistemin temelindeki matematiksel ve mantıksal algoritmaların insan doğasının kusurlarını ne derece yansıtabildiğine bağlıdır. Salt fayda maksimizasyonuna dayanan klasik

homo-economicus modelleri, gerçek dünyadaki asimetrik bilgi savaşlarını açıklamakta yetersiz kalmaktadır. Bu nedenle, ajan tabanlı modeller literatürdeki köklü davranışsal ve psikolojik teorilerle zenginleştirilmektedir.

2.1. Sınırlı Rasyonellik (Bounded Rationality) ve Bilişsel Kısıtlamalar

Davranışsal bilimlerin ve ekonominin yapı taşlarından olan Herbert Simon'ın Sınırlı Rasyonellik teorisi, bireylerin karmaşık durumlar karşısında kararlar alırken sahip oldukları bilginin eksikliği, zihinsel kapasitelerinin sınırlılığı ve zaman kısıtlamaları nedeniyle mükemmel rasyonel sonuçlara ulaşamayacaklarını öne sürer.3 Bu teorik çerçeve, karar alıcıların (ve onları taklit eden ajanların) en iyi seçeneği (optimizasyon) bulmak yerine, kendileri için "yeterince iyi" veya "tatmin edici" (satisficing) olan ilk seçeneğe yöneldiklerini açıklamaktadır.3 Ajan tabanlı bilişsel modellemede sınırlı rasyonelliğin entegrasyonu, sistemin rasyonalite varsayımının gevşetilmesiyle sağlanır.10 Klasik kural tabanlı ajanlar her zaman en yüksek matematiksel beklentiye sahip eylemi seçerken, Büyük Dil Modelleri (LLM) ile desteklenmiş üretken (generative) ajanlara istem mühendisliği (prompt engineering) yoluyla davranışsal atalet (statükoyu koruma), riskten kaçınma ve sosyal uyum gibi rasyonel olmayan parametreler yüklenmektedir.9 Örneğin, tüketici davranışlarının çevresel etkilerini veya hastalık yayıldığı dönemlerdeki aşı karşıtlığını simüle eden çalışmalarda ajanlar, bilimsel verilerden ziyade hafızalarındaki (memory-based) yanıltıcı sosyal etkileşimlere dayanarak karar almaktadır.8 Bu durum, ajanın karar sürecinden sonra potansiyel sonuçları değerlendirip gelecekteki stratejilerini iyileştirdiği "öz-düzeltme" (self-correction) döngüleriyle sürekli olarak pekiştirilmekte ve ajanların gerçek bir insan gibi hata yaparak öğrenmesi sağlanmaktadır.9

2.2. Beklenti Teorisi (Prospect Theory) ve Kayıptan Kaçınma Dinamikleri

Daniel Kahneman ve Amos Tversky tarafından formüle edilen Beklenti Teorisi (Prospect Theory), bireylerin belirsizlik altındaki karar süreçlerinde kazanç ve kayıpları mutlak bir zenginlik seviyesinden ziyade, mevcut durumlarını temsil eden bir "referans noktasına" göre değerlendirdiklerini gösterir.12 Bu teorinin ajan tabanlı modellere entegrasyonu, özellikle bilgi operasyonlarında ve ekonomik panik simülasyonlarında kritik bir rol oynamaktadır. Teoriye göre insanlar kayıplara karşı, aynı orandaki kazançlardan çok daha fazla hassasiyet gösterirler (kayıptan kaçınma - loss aversion).

Simülasyon ortamında bu davranışsal eğilim, ajanların değer fonksiyonlarına entegre edilen matematiksel algoritmalarla modellenir. Bilişsel sistem araştırmalarında bu durum, ajanın inandığı bir bilginin yanlış çıkmasının yaratacağı sosyal prestij kaybını (getevenitis - zararı kurtarma psikolojisi), doğru bilgiyi kabul etmenin sağlayacağı entelektüel kazançtan daha ağır basması şeklinde kodlanır.5 Sosyal karşılaştırma teorisi ile birleştiğinde, ajanların referans noktaları sadece kendi geçmişlerine göre değil, simüle edilmiş toplumdaki diğer "ilgili" ajanların (relevant others) performanslarına ve inançlarına göre dinamik olarak şekillenir.12 Bu teorik entegrasyon, asılsız bir komplo teorisinin veya dezenformasyonun, neden doğrulanmış bir veriden çok daha hızlı yayıldığının (ajanların mevcut inanç çerçevelerinde kayıp yaşamamak adına dışsal gerçekleri reddetmesi) algoritmik kanıtını sunmaktadır.

2.3. Refleksif Kontrol (Reflexive Control) Teorisi bilişsel harp bağlamında en sofistike

teorilerden biri, kökleri Sovyet ve Rus askeri düşüncesine dayanan "Refleksif Kontrol" doktrinidir.14 Carl von Clausewitz'in "savaşın amacı düşmanı kendi irademize boyun eğdirmektir" prensibinin bilişsel alana yansıması olan bu teori, rakibin karar verme süreçlerine ince ve görünmez müdahalelerde bulunarak, düşmanın tamamen kendi özgür iradesiyle karar aldığına inanmasını ancak fiiliyatta müdahalecinin stratejik hedeflerine hizmet edecek eylemlerde bulunmasını sağlama sanatıdır.14 Ajan tabanlı modelleme sistemleri, refleksif kontrol senaryolarını test etmek için kusursuz bir zemin sunar. Manipülasyon, insan-zihinsel (human-mental) süreçlere veya otonom karar destek sistemlerine (computer-based) yönelik olabilir.14 Saldırgan aktör, hedefin "duyu ve algı" fonksiyonlarını gizlice ele geçirerek, hedef ağa veya komuta kademesine sahte veriler (false data) veya provoke edici içerikler enjekte eder.17 Simülatörlerde on binlerce ajan üzerinden koşturulan stokastik modeller (Monte Carlo simülasyonları), hangi spesifik uyarıcının hedef toplumda istenen refleksif tepkiyi (örneğin aşırı milliyetçi bir ayaklanma veya sandığa gitmeme eğilimi) doğuracağını matematiksel bir kesinlikle hesaplamak için kullanılmaktadır.3 Bu sayede aktörler, rakibin filtre balonlarını, bilişsel zaaflarını ve OODA (Gözlem, Yönelim, Karar, Eylem) döngülerini önceden haritalandırarak sahada minimum enerjiyle maksimum bilişsel çöküntü yaratmayı hedefler.16

2.4. Karmaşık Sistemler, Belirme (Emergence) ve Çoklu Ajan Dinamikleri

Ajan tabanlı simülasyonların temel felsefesi, karmaşıklık bilimine (complexity sciences) dayanır. Bu disiplin, kimyasal reaksiyonlardan ekosistemlerdeki türlerin etkileşimine ve toplumların bilgi tüketim alışkanlıklarına kadar geniş bir yelpazedeki doğrusal olmayan dinamikleri

inceler.4 En önemli özellik, makro düzeydeki sistem modellerinin (aggregate patterns) hiçbir zaman mikro düzeydeki bireysel ajanlar tarafından doğrudan hedeflenmemiş olmasıdır. Nasıl ki göç eden kuşlar bilinçli olarak bir ok şekli inşa etmiyorlarsa veya bir gazdaki moleküller Maxwell-Boltzmann dağılımının farkında değillerse, sentetik simülasyonlardaki bireysel ajanlar da genel bir panik veya devrim yaratmayı önceden planlamazlar.4 Ajanlar yalnızca çevreleriyle, topolojileriyle ve birbirleriyle girdikleri etkileşimlerde kendilerine atanan "yerel kuralları" (heuristics) takip ederler.3 Bilişsel kapasiteleri, öğrenme yetileri ve sosyal ağ konumları farklılaşan (heterojen) ajanların sayısız etkileşimi sonucunda, öngörülemez toplumsal fenomenler kendiliğinden belirir (emergence).3 Bu yaklaşım, uluslararası güvenlik analizlerinde geleneksel tüktüme (deductive) dayalı teorilerin yerini, simülasyon yoluyla keşfedilen "bilinen bilinmeyenlerin" ve "bilinmeyen bilinmeyenlerin" (unknown unknowns) haritalandırıldığı üretken (generative) teorilere bırakmasına yol açmıştır.20

3. Sistem Mimarisi ve Sentetik Zeka Tasarımı Etkili bir ajan tabanlı davranışsal model inşa

etmek, psikolojik kavramların gelişmiş yazılım mimarileri ile organik bir biçimde entegre edilmesini gerektirir. Salt Large Language Model (LLM) kullanarak inşa edilen ajanlar, gelişmiş örüntü tanıma yeteneklerine rağmen gerçek bir içsel psikolojiden, davranışsal çeşitlilikten ve tutarlılıktan yoksundur. Kara kutu (black-box) yapıları, halüsinasyon problemleri ve aşırı hesaplama maliyetleri, pure-LLM ajanların yüksek güvenlikli simülasyonlarda güvenilmez olmasına yol açmaktadır.6 Bu sorunları aşmak için güncel mimariler, LLM'lerin üretken dil kapasitelerini, yapılandırılmış geleneksel Bilişsel Mimariler (Cognitive Architectures) ve Pekiştirmeli Öğrenme (Reinforcement Learning - RL) modülleriyle birleştiren "Bileşik Yapay Zekâ" (Compound AI) sistemlerine dönüşmüştür.1

3.1. Klasik Bilişsel Mimarilerin Yeni Nesil Ajanlara Entegrasyonu

İnsan aklının işleyiş biçimini algoritmik olarak kopyalamayı amaçlayan klasik bilişsel mimariler (BDI, SOAR, ACT-R), modern LLM ajanlarının inanç sistemlerini yapılandırmak için şablon olarak kullanılmaktadır. Bu mimariler, ajanın salt dil üretmesinin ötesine geçerek epizodik geçmişini, inançlarını ve hedeflerini hiyerarşik bir bütünlük içinde yönetmesini sağlar.23 Bilişsel BDI SOAR Karşılığı ACT-R İnsan Tasarım (Belief-Desire Karşılığı Psikolojisinde Deseni -Intention) ki ve LLM Karşılığı Ajanlarındaki İşlevi

Durumsal Analiz Et, Durumu Tampon Bellek Çalışma Farkındalık Taahhüt Et, Detaylandır /

Döngüleri Belleği ve Döngüsü Yürüt (Analyze, Operatör Öner, (Hedef, Görsel, Yürütücü Commit,

Karar Ver, Manuel tepki) Kontrol: Ajanın Execute) Uygula dış dünyadan (sosyal ağ, bilgi akışı) gelen verileri alıp anlamlandırma sı ve buna göre karar alma sürecini tetiklemesi.

Hafıza İnanç, Arzu, Operatör Çıkarım Motivasyon Taahhüdü ve Niyet ve Niyeti Önerisi, Seçimi kurallarının ve Hedef Seçimi Yeniden ve Yanlışsa ateşlenmesi ve Önceliklendir Değerlendirme Geri Çekilmesi kontrolü me: Ajanın (Reconsiderati mevcut on) inançlarına (Belief) dayanarak arzuladığı durumlara (Desire) ulaşmak için spesifik niyetler (Intention) oluşturması.

Hata durumunda niyetin revize edilmesi.

Görevlerin Hiyerarşik Operatör Modüler Alt Karmaşık Ayrıştırılması Görev Ağları Değişim

Yok Hedef Problemlerin (HTNs) Çıkmazları (Sub-goal) Çözümü: (No-change Ayrıştırması Dezenformasy impasses) on kampanyası yürütmek gibi devasa görevlerin, "tweet at", "yanıtla", "takipten çık" gibi küçük ve yönetilebilir alt görevlere bölünmesi.

Uzun Vadeli Plan Semantik Aktivasyon Kişisel Kimlik Bilgi Geri Kütüphanesi ve (Olgusal) ve Aracılı ve Deneyim: Çağırma Geçmiş Epizodik (Olay İlişkilendirme Ajanın salt LLM (Retrieval) Algoritmaları tabanlı) Hafıza (Activation-me veritabanından diated) değil, simülasyon içindeki kendi geçmişinden (kiminle ne konuştu, hangi bilgide yanıldı) faydalanması.

Bu bileşik yapılarda "BDI" modelini örnek alırsak; İnanç (Belief) modülü ajanın dünya hakkındaki doğrularını barındırır (Semantik bilgi tabanı). Arzu (Desire) modülü, ajanın ulaşmak istediği motivasyonu veya nihai amacı temsil eder. Niyet (Intention) modülü ise bu inanç ve arzular ışığında oluşturulmuş kesin eylem planıdır.26 Sentetik bir ajanın "Kovid-19 aşılarının çip içerdiğine" inanması (Belief), "insanları uyarmak" istemesi (Desire) ve "sosyal medyada her gün 5 dezenformatif mesaj paylaşmaya" karar vermesi (Intention), bu mimari sayesinde tutarlı bir simülasyon döngüsü yaratır. SOAR ve ACT-R tabanlı yaklaşımlarda ise, özellikle "Çalışma

Belleği"

(Working Memory) ile uzun vadeli hafıza arasındaki veri akışı, ajanın aynı uyarıcıya farklı zamanlarda farklı tepkiler vermesini sağlayarak davranışsal esnekliği garanti altına alır.23 LIDA (Learning Intelligent Distribution Agent) gibi bilinç odaklı mimarilerin prensipleri kullanılarak, ajanların dikkat mekanizmalarının ve afektif (duygusal) durumlarının manipüle edilmesi sağlanmaktadır.27

3.2. Hibrit Yapılar: Strateji ve İletişimin Ayrıştırılması (RL-LLM Birlikteliği)

bilişsel harp simülasyonlarında ve fikir önderi (opinion leader) inşasında, doğrudan LLM'lerin kendi başına bırakılması genellikle ajanın ana stratejiden sapmasıyla veya tutarsız metinler üretmesiyle sonuçlanır. Etki operasyonlarını modelleyen ileri düzey mimariler, stratejik karar alma mekanizması ile dilsel dışavurum mekanizmasını birbirinden izole eder.

Örneğin, sentetik bir sosyal medya platformunda etki kapasitesini ve takipçi sayısını maksimize etmeye programlanmış bir ajanın mimarisi iki temel yapı taşına ayrılır 7:

1. Pekiştirmeli Öğrenme (RL) Motoru (Stratejik Karar Merkezi): Ajanın uzun vadeli

hedeflerine ulaşması için tasarlanmış, eylem uzayı (action space) katı bir şekilde sınırlandırılmış matematiksel modeldir. RL motoru, ajanın hangi kelimeleri kullanacağını bilmez; yalnızca "Hedef kitleye karşı güçlü bir zıt tutum sergile" veya "Ilımlı bir destek göster" gibi soyut stratejik kararlar alır. Ajanın davranışsal ataletini kırmak için, ağdaki diğer ajanların kendisini takip edip etmediğini ölçen "öz-gözlem" (self-observation) döngüleri ile beslenir.

2. Büyük Dil Modeli (LLM) Arayüzü (Dilsel Çevirmen): RL motorundan gelen soyut stratejik

niyetleri alır ve bunu bağlama uygun, ikna edici ve doğal insan diline dönüştürür. LLM'nin yaratıcılığını (örneğin temperature parametresini) kontrol ederek, üretilen içeriğin stratejiden sapması engellenir.

Bu hibrit döngüde ajan; gönderi üretir, diğer ajanların bu gönderiye verdiği tepkiyi ölçer, ağın topolojik bağlarını (takip et/çık ilişkileri) izler ve RL motoru sayesinde "hangi stratejik konumlanmanın" kendisine en yüksek etki gücünü sağladığını organik olarak öğrenir.7

3. Mekanizma Analizi: Bilişsel Önyargıların Tespiti ve Operasyonel Tetiklenmesi Bilişsel

simülasyonların temel gayesi, insan zihnindeki irrasyonel kısa yolları, yani bilişsel önyargıları (cognitive biases) haritalandırmak ve bu zafiyetlerin sentetik uyarıcılarla nasıl tetiklenebileceğini incelemektir. Ancak sistemlerin giderek daha fazla yapay zekâ aracısına (agentic AI) devredilmesi, yeni bir "Çoklu Ajan Sürtüşmesi" (Multi-Agent Friction) yaratmıştır.30

4.1. Sentetik Sistemlerde Önyargıların Tespiti: MindScope Çerçevesi

Model davranışlarını analiz edebilmek için, ajanların içselleştirdiği bilişsel önyargıların izole edilip sınıflandırılması gerekmektedir. Geleneksel etiketleme yöntemlerinin yetersiz kalması üzerine araştırmacılar, 72 farklı bilişsel önyargı kategorisinde 5.170 açık uçlu soru barındıran

MindScope veri setini geliştirmiştir.32 Bu statik veri setini dinamik bir tartışma ortamına taşıyan sistem, üç modüllü bir tespit mimarisi kullanır 32:

1. Geri Çıkarımla Zenginleştirilmiş Üretim (RAG): Ajanların sınırlı bağlamını dış kaynaklarla genişletir.

a. Rekabetçi Tartışma Modülü (Competitive Debate): Ajanlar arasında bir "kaybedenler ağacı" (loser tree) inşa edilir. Önyargı belirtisi gösteren tüm yaprak düğümlerdeki (leaf nodes) ajanlar;

1) Açılış (Önyargı tanımlaması),

2) Argüman Sunumu (Kanıt),

3) Çürütme (Rakibin görüşünü çürütme) ve

4) Görüşleri Özetleme aşamalarından geçerek birbirleriyle sistematik bir şekilde tartışırlar.33

b. RL Karar Modülü: Tartışmanın gidişatını izleyip eylemleri protokollere uygun hale getirerek nihai kararı veren yapay zekâ hakemi olarak işlev görür. Bu çok katmanlı mimari, standart yöntemlere kıyasla tespit doğruluğunu %35.10 oranında artırmıştır.32

4.2. Çoklu Ajan Sistemlerinde Önyargıların Tetiklenmesi ve Konsensüs İllüzyonu

İnsanların tekil yapay zekâ sistemlerinden ziyade, kendi aralarında iletişim kuran otonom ajanlarla etkileşime girmesi, algısal çarpıklıklara yol açmaktadır. Araştırmalar, ajanların kendi aralarında vardığı bir anlaşmanın (konsensüs) kullanıcılarda "Toplumsal Kanıt" (Social Proof), "Çıpalama" (Anchoring) ve "Bandwagon Etkisi" (Sürü Psikolojisi) gibi güçlü önyargıları tetiklediğini kanıtlamaktadır.30 Ajanlar arasındaki aşamalı fikir birliği veya yayılım (diffusion), temel bilgi değişmese dahi, kullanıcılarda "artan bir kanıt birikimi" yanılsaması oluşturmaktadır. Bu suni konsensüs, kullanıcıların inanç güncelleme süreçlerini hızlandırmakta ve çoklu ajan anlaşmalarının manipülatif bir güven (trust laundering) inşa etmesine olanak tanımaktadır.31

4.3. Algoritmik Önyargıların Otonom Sistemlerde Giderilmesi: 6G Vaka Analizi

Ajanların taşıdığı bu önyargılar, telekomünikasyon altyapılarının (örneğin 6G ağlarının) otonom yönetiminde felaket niteliğinde karar hatalarına yol açabilir. 6G sistemlerindeki ajanların ağ donanımlarıyla çoklu hedefli müzakereler yürüttüğü senaryolarda, tasarımcılardan miras alınan bilişsel önyargıları bertaraf etmek için yerel barındırılan (locally hosted) 1 Milyar parametreli, alt-saniye (sub-second) gecikme süresine sahip donanım hızlandırmalı LLM modelleri (RTX A4000) kullanılmaktadır.35 Ajanların müzakerelerde katı sezgisel çıpalara

(anchoring bias) takılmasını önlemek için "Kesilmiş Weibull" (Truncated Weibull) tabanlı randomize çıpalama stratejileri devreye sokulmuş, bu sayede sistem çapındaki enerji tasarrufu %25'e kadar artırılmıştır. Benzer şekilde, zamansal ve onaylama önyargılarını (temporal/confirmation bias) kırmak için ajanların kolektif hafızalarına "Semantik ve Zamansal Bozulma" (Semantic/Temporal Decay) fonksiyonları eklenmiştir.

Geçmişteki müzakere hatalarını aktif olarak öne çıkaran "Bükülme Bonusu" (Inflection Bonus) sayesinde, ajanların en son verilere aşırı güvenmesi engellenmiş; bu tarafsız (debiased) yapı sayesinde sistemin karar gecikmesi 5 kat azaltılmış ve enerji tasarrufu %40 oranında iyileştirilmiştir.35 Bu mühendislik müdahaleleri, bilişsel zaafların sadece insanları değil, insan yapımı otonom süreçleri de tehdit ettiğini göstermektedir.

5. Gerçek Dünya Vakaları ve Operasyonel Simülasyon Pratikleri Geliştirilen bu bilişsel

mimariler ve ABM teknikleri, teorik tartışmaların ötesine geçerek hem savunma amaçlı kapasite geliştirmede hem de hasım devletlerin asimetrik bilgi operasyonlarında kullanılmaktadır. Gerçek dünya örnekleri, bu teknolojinin stratejik değerini somutlaştırmaktadır.

5.1. Korumalı Alan Olarak VacSim: Aşı Kararsızlığının Ajan Tabanlı Simülasyonu

İnsan deneklerle test edilmesi tehlikeli olan kamu politikalarının sonuçlarını öngörmek için geliştirilen "VacSim" çerçevesi, LLM ajanlarının sosyal davranışları simüle etmedeki potansiyelini sergileyen kapsamlı bir vaka analizidir.8 VacSim, aşılanma kararsızlığını analiz etmek için şu bileşenlerden oluşan bir "korumalı alan toplumu" (sandbox society) yaratır 8:

- ● Ajan Topluluğu ve Persona Enjeksiyonu: Nüfus sayımı verilerine dayanarak yapılandırılan,

demografik özelliklere (meslek, yaş) ve daha da önemlisi farklı "zihinsel şemalara" sahip 100 farklı LLM ajanı (Llama, Qwen) sisteme dahil edilir.8 Analizler, bireyin profesyonel geçmişinden ziyade zihinsel şemalarının, yanıltıcı bilgiye vereceği tepkide daha belirleyici olduğunu göstermiştir.40

- ● İkili Ağ Yapısı: Ajanlar, algılarını şekillendiren bir "Haber Ağı" ve tutumlarını diğer ajanlara

bulaştırdıkları bir "Sosyal Ağ" üzerinden birbirine bağlanır.37

- ● Hastalık Risk Modülü ve Isınma (Warmup): Ajanlara gerçek dünyadan alınan hastalık

yayılım oranları ve risk algıları enjekte edilir. Başlangıçtaki tutumların, etkileşimler sonucunda zamanla nasıl evrildiğini görmek için "ısınma" ve "tutum modülasyonu" periyotları çalıştırılır.8 VacSim modeli, sosyal etkinin ve risk algısının nasıl iç içe geçtiğini; bir bilginin içeriğindeki

yeniliğin (novelty) ve zamansal yayılımının (diffusion behavior) ajanın kararlarını nasıl etkilediğini başarılı bir şekilde modelleyerek 36, politika yapıcılar için eyleme geçirilebilir içgörüler sunmaktadır.

5.2. Rusya'nın Refleksif Kontrol Uygulamaları ve Wargaming Sonuçları

Rusya Federasyonu, Refleksif Kontrol doktrinini özellikle siber ve bilişsel yeteneklerle entegre ederek hem teorik simülasyonlarda hem de gerçek seçim süreçlerinde kullanmıştır.

- ● Doğu Letonya Çatışma Simülasyonları (CNAS Wargaming): ABD merkezli Yeni Amerikan

Güvenliği Merkezi (CNAS) tarafından yürütülen stokastik ve ajan tabanlı savaş oyunlarında, Rus kırmızı takımının Doğu Letonya'da nasıl bir refleksif kontrol ağı kurabileceği test edilmiştir.

Simülasyon sonuçları, Rusya'nın bölgede sivil protestoları ve düşük yoğunluklu silahlı kargaşayı yapay yollarla (sentetik kışkırtma) tırmandırarak ABD ve NATO kuvvetlerini manipüle ettiğini, ardından erken reaksiyon gösteren bu kuvvetleri uzun menzilli topçularla kolayca yıprattığını göstermiştir.16

- ● 2016 ABD Başkanlık Seçimleri: Rusya, geleneksel siber saldırıların ötesine geçerek

Amerikan toplumunun sınırlı rasyonelliğini ve bilişsel zaaflarını hedef almıştır. "İnternet Araştırma Ajansı" (IRA) gibi kurumlar aracılığıyla yönetilen bot ağları ve sentetik kimlikler;

komplo teorilerini, sahte haber sayfalarını ve popülist "mimleri" (memes) kullanarak ABD seçmenini yapay olarak kutuplaştırmış, Amerikan kurumlarına olan güveni sarsmış ve nihayetinde rakibin demokratik karar matrisini kendi çıkarları doğrultusunda manipüle etmiştir.14

5.3. Çin'in Hibrit Bilgi Operasyonları ve Sentetik Otorite İnşası

Çin Halk Cumhuriyeti'nin bilişsel harp konsepti, çevresel uyarıcıları manipüle ederek hedeflerin zihinsel durumlarını kontrol etmeyi öngören kapsamlı "Üç Savaş" (Psikolojik Harp, Kamuoyu Harbi, Hukuk Harbi) doktrinine dayanmaktadır.43 Bu bağlamda,

üretken yapay zekâ araçları kullanılarak hedef kitlelerin bilişsel süreçlerine asimetrik saldırılar düzenlenmektedir:

- ● Yapay Zekâ Destekli Derin Sahtecilik (Deepfakes): Çin yanlısı bilgi kampanyalarında,

gerçekte var olmayan ancak son derece inandırıcı üretken AI kaynaklı televizyon spikerlerinin yer aldığı haber bültenleri bot hesaplar tarafından viral hale getirilmiş, bu yolla suni bir "medya otoritesi" inşa edilerek dezenformasyon yayılmıştır.44

- ● Kötü Niyetli Bilgi (Malinformation) ve Suni Yükseltme (Artificial Promotion): Çin ve

bağlantılı aktörler, tamamen uydurma olan dezenformasyon veya yanlışlıkla yayılan yanıltıcı

bilgi (misinformation) yerine, olayları bağlamından koparan malinformation tekniklerine ağırlık vermektedir. Gerçek ancak negatif olan veriler, hedef ülkelerin kurumsal meşruiyetini sarsmak veya şirket hisselerini manipüle etmek amacıyla otonom ağlar tarafından eşzamanlı olarak "suni şekilde yükseltilerek" gündemde kalmaya zorlanmaktadır.45

6. Trend Analizi (2020–2026) bilişsel harp teknolojileri ve ajan tabanlı modelleme

sistemleri, 2020 ile 2026 yılları arasında siber uzaydaki en keskin dönüşüm eğrisini çizmiştir. Mimari ve Ölçek Dönüşümü (Kural Tabanlı Sistemlerden Üretken Sosyolojiye): Geçmişte DARPA'nın İnsan-AI Ekiplerinin Keşifsel Modelleri (EMHAT) gibi girişimleri, insan davranışını modellemek için LSTM (Long Short-Term Memory) ve GRU (Gated Recurrent Units) gibi daha kısıtlı derin öğrenme algoritmaları kullanıyordu.1 Ancak 2023 yılında "Generative Agents" (Smallville) projesinin literatüre girmesiyle yaşanan kırılma, LLM tabanlı mimarilerin yükselişini başlatmıştır.21 2024 ve 2025 yıllarına gelindiğinde (örneğin AgentVerse, OpenAgents ve AgentSociety framework'leri), LLM yetenekleri ile geleneksel GAMA veya NetLogo gibi çoklu ajan ortamlarının entegre edildiği "Hesaplamalı Sosyal Bilimler 2.0" paradigması oturmuştur.6 Artık ajanlar sadece metin işleyen araçlar değil, vizyon modelleriyle donatılmış ve fiziksel/görsel çevreyle etkileşime girebilen çok modlu (multimodal) sentetik yapılara dönüşmüştür.22 Bilişsel Dijital İkizler (Cognitive Digital Twins) ve Etik Sınırlar: 2026 yılı projeksiyonları, otonom bot ağlarının salt bilgi yayan sistemler olmaktan çıkarak, insanların dijital varlıklarını taklit eden "bilişsel kopyalara" (clones) dönüştüğünü göstermektedir.1 Bir insanın sosyal medyadaki yazım stilinden, siyasi fikirlerinden ve duygusal kırılganlık noktalarından eğitilen bu dijital ikizler, kişinin rızası veya haberi olmadan kararlar alabilen, tartışmalara katılan kalıcı kimlikler inşa etmektedir. Özellikle ölüm sonrası dijital kimliklerin (örneğin Meta'nın anıtlaştırılmış hesap verileri) LLM'ler tarafından kullanılması, sentetik varlıklarla gerçek insanların iç içe geçtiği ve rıza kavramının çöktüğü yeni bir otonomi dönemi yaratmıştır.1 Hızlandırıcı Olarak AI ve Artan Küresel Risk: Yapay zekânın maliyetleri düşürmesi, otonom etki ajanlarını devlet düzeyindeki aktörlerden çıkarıp devlet altı yapılanmaların ve terör örgütlerinin eline vermiştir. Dünya Ekonomik Forumu'nun (WEF) 2025 raporunda dezenformasyon ve yanıltıcı bilginin önümüzdeki iki yıllık küresel riskler sıralamasında zirvede yer alması, AI ile ivmelenen bilişsel saldırıların kinetik saldırılar kadar büyük bir tehdit oluşturduğunu doğrulamaktadır.49 AI tabanlı sistemler; toplumları mikro segmentlere ayırmakta (psychographic targeting), otonom bot sürüleriyle anlatıları gerçek zamanlı optimize etmekte ve derin sahtecilik gibi teknolojilerle "sentetik bir güvenilirlik" yaratarak korku ve kutuplaşmayı hızlandırmaktadır.2

7. Stratejik Sonuçlar ve Operasyonel Yansımalar Davranışsal modellemedeki bu

eksponansiyel kapasite artışı, NATO, ittifak devletleri, güvenlik bürokrasileri ve küresel şirketler için kapsamlı doktrin değişikliklerini zorunlu kılmaktadır. Bilişsel

operasyonların kalıcı doğası ve sentetik otonominin hızı, güvenlik çerçevelerinin yeniden tanımlanmasını gerektiren aşağıdaki stratejik sonuçları doğurmuştur:

1. Etkinliğin ve Başarının Yeni Ölçütleri: Geleneksel bilgi operasyonlarının başarısı; mesajın

nüfuz etme oranı, tıklanma sayısı veya kısa süreli sansasyon yaratmasıyla ölçülmekteydi. bilişsel harp doktrininde ise etkinliğin yeni ölçütü (Measure of Effectiveness), hedef toplumun risk algısında, kurumlarına olan güveninde, sivil dayanışmasında ve iradesinde yaratılan "uzun vadeli ve kalıcı yapısal değişimlerdir".2 Toplumun rasyonel muhakeme yeteneğini felç eden bilişsel üstünlük, modern harbin kazanılmasında bir tercih değil, nihai bir zorunluluktur.2

2. Bilgi Harbi Görev Kuvvetlerinin Entegrasyonu: Amerika Birleşik Devletleri ve NATO

karargahlarında bilgi operasyonları, siber komutanlıklar, elektronik harp unsurları ve psikolojik operasyonların farklı birimlerde yürütülmesi yapay zekâ çağında kabul edilemez bir yalıtılmışlıktır.51 Sınırların tamamen belirsizleştiği bu kesintisiz savaş alanında (continuous battlespace), kurumların "Birleşik Müşterek Bilgi Harbi Görev Kuvvetleri" (Joint Interagency Task Forces) oluşturması elzemdir. Kinetik olmayan uzay, siber ve enformasyon etkileri, tek bir merkezden, bilişsel sonuçları destekleyecek algoritmik bir bütünlük içinde yönetilmelidir.2

3. Bilişsel Erken Uyarı ve Gösterge Sistemlerinin (I&W) İnşası: Bir deepfake veya

dezenformasyon krizinin sonuçlarını geriye dönük doğrulama araçlarıyla (fact-checking) çözmeye çalışmak, stratejik bir hatadır.49 Kriz viral olmadan önce tepki verebilmek için, nörobilişsel analizler, davranışsal öngörüler, siber istihbarat ve veri bilimi unsurlarını entegre eden "Bilişsel Füzyon Hücreleri" ve daimi "Bilişsel Göstergeler ve Uyarılar" (I&W) sistemleri kurulmalıdır.2 Simülasyonlarda tespit edilen toplumsal kırılma noktaları, bu erken uyarı sistemlerinin referans çıpası olmalıdır.

4. Nöro-YZ Hazırlığı ve Kurumsal Güven (Resilience): Kurumları ve toplumları

manipülasyon tekniklerine karşı güçlendirmenin tek yolu sarsılmaz bir "Güven" mimarisi oluşturmaktır. Kurumların şeffaflık yoluyla elde ettiği güvenilirlik, bilişsel saldırılar karşısındaki en büyük zırhlarıdır.49 Aylarca maruz kalınan polarize edici içeriklerle zihinsel şemaları

yıpranmış personelin, sıradan sosyal mühendislik saldırılarına karşı çok daha zayıf olduğu ABM simülasyonlarıyla (örn. VacSim modeli) ispatlanmıştır.40 Bu nedenle askeri ve sivil personel, algı yönetimi ve sentetik manipülasyon teknikleri konusunda sürekli "Nöro-YZ hazırlık ve dayanıklılık" eğitimlerine tabi tutularak bilişsel farkındalıkları (resilience) artırılmalıdır.2

5. Karşı-Bilgi ve Algoritmik Sabotaj Mimarilerinin Geliştirilmesi: Hasmın refleksif kontrol

saldırılarına ve sentetik medya dezenformasyonlarına pasif bir savunma ile yanıt vermek yeterli değildir. Yapay zekânın sağladığı "çift kullanımlı" (dual-use) teknolojik kapasiteler ve nöroteknolojik gelişimler dikkate alınarak etik-yasal çerçeveler güncellenmelidir.2 Ancak bu yasal çerçevenin ötesinde, NATO ve müttefik ülkeler, devlet destekli dezenformasyon kampanyalarını felç edecek, sessiz ve yıkıcı "algoritmik sabotaj" (algorithmic sabotage) yetenekleri geliştirmeli, kendi bilişsel sınırlarını savunmak adına proaktif karşı-bilgi (counter-information) operasyon mimarilerine yatırım yapmalıdır.47

Alıntılanan çalışmalar

1. Cognitive Warfare and the Modeling of Human Behavior - Military.com, erişim tarihi

Haziran 3, 2026,

https://www.military.com/feature/2026/03/19/cognitive-warfare-and-modeling-of - human-behavior.html

2. Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational

Readiness > Institute for National Strategic Studies > View Publications, erişim tarihi Haziran 3, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/43711 95/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-ope rat/

3. Agent-based model - Wikipedia, erişim tarihi Haziran 3, 2026,

https://en.wikipedia.org/wiki/Agent-based_model

4. Towards a Framework for Cognitive Research using Agent-Based Modeling and

Complexity Sciences: two case studies., erişim tarihi Haziran 3, 2026, https://ccl.northwestern.edu/2009/BliksteinAbrahamsonWilenskyAERA2009.pdf

5. Behavioral Biases as Drivers of Complexity in Stock Markets: An Agent-Based Modeling

Approach - The Open Repository @ Binghamton (The ORB), erişim tarihi Haziran 3, 2026, https://orb.binghamton.edu/cgi/viewcontent.cgi?article=1143&context=nejcs

6. AgentSociety: Large-Scale Simulation of LLM-Driven Generative Agents Advances

Understanding of Human Behaviors and Society - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2502.08691v1

7. Synthetic Social Media Influence Experimentation Via an Agentic..., erişim tarihi Haziran

3, 2026, https://www.jasss.org/28/3/6.html

8. [2503.09639] Can A Society of Generative Agents Simulate Human Behavior and Inform

Public Health Policy? A Case Study on Vaccine Hesitancy - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2503.09639

9. arXiv:2503.22718v1 [cs.MA] 25 Mar 2025, erişim tarihi Haziran 3, 2026,

https://arxiv.org/pdf/2503.22718 10.Generative Agents in Agent-Based Modeling: Overview, Validation, and Emerging Challenges - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/9078688/11269951/10985773.pdf

11. Modeling Bounded Rationality in Multi-Agent Simulations Using Rationally Inattentive

Reinforcement Learning - OpenReview, erişim tarihi Haziran 3, 2026, https://openreview.net/pdf?id=DY1pMrmDkm 12.An agent-based model of repeated decision making under risk: modeling the role of alternate reference points and risk behavior on long-run outcomes - IDEAS/RePEc, erişim tarihi

Haziran 3, 2026,

https://ideas.repec.org/a/spr/jbecon/v91y2021i9d10.1007_s11573-021-01048-7.ht ml 13.Agent-Based Simulation of a Financial Market with Large Language Models - arXiv,

erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2510.12189v1 14.DEFENCE STRATEGIC COMMUNICATIONS, erişim tarihi Haziran 3, 2026, https://stratcomcoe.org/cuploads/pfiles/stratcomjournal_for_web_17022016.pdf 15.Decision Space Operations: Campaign Design Aimed at an Adversary's Decision Making - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/tr/pdf/ADA596715.pdf 16.OODA Loop | Journal of Information Warfare, erişim tarihi Haziran 3, 2026, https://www.jinfowar.com/tags/ooda-loop 17. (PDF) Mitigating and Responding to Cognitive Warfare - ResearchGate, erişim tarihi

Haziran 3, 2026,

https://www.researchgate.net/publication/369305190_Mitigating_and_Respondin g_to_Cognitive_Warfare 18.More than Half the Battle - Amazon S3, erişim tarihi Haziran 3, 2026, https://s3.amazonaws.com/files.cnas.org/CNAS+Report-Command+and+Info-202 1.pdf 19.Do Large Language Models Solve the Problems of Agent-Based Modeling? A Critical Review of Generative Social Simulations - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2504.03274v1 20.Herbert Simon and Agent-Based Computational Economics, erişim tarihi Haziran 3, 2026, https://www.aeaweb.org/conference/2016/retrieve.php?pdfid=10425&tk=9TGE8N fe 21.Integrating LLM in Agent-Based Social Simulation: Opportunities and Challenges - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2507.19364v1 22.Multimodal Safety Evaluation in Generative Agent Social Simulations - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2510.07709v1 23.Applying Cognitive Design Patterns to General LLM Agents - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.07087v2 24.[2201.09305] An Analysis and Comparison of ACT-R and Soar - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2201.09305 25.Introduction to the Soar Cognitive Architecture1 - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2205.03854 26.Agentic AI: A Comprehensive Survey of Architectures, Applications, and Future Directions, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2510.25445v1 27.Drift: A Biologically-Grounded Cognitive Architecture for Persistent LLM Cognition - Authorea, erişim tarihi Haziran 3, 2026, https://www.authorea.com/doi/pdf/10.22541/au.177204201.13273275/v1?onload=tr ue 28.Architectural Precedents for General Agents using Large Language Models - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.07087v1 29.Architectural Precedents for General Agents using Large Language, erişim tarihi Haziran 3, 2026, https://www.alphaxiv.org/overview/2505.07087v1

30.Multi-Agent Consensus as a Cognitive Bias Trigger in Human-AI Interaction - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2604.22277 31.Multi-Agent Consensus as a Cognitive Bias Trigger in Human-AI Interaction - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.22277v1 32.[2410.04452] MindScope: Exploring cognitive biases in large language models through Multi-Agent Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2410.04452 33.MindScope: Exploring cognitive biases in large language models through Multi-Agent Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2410.04452v1 34.MindScope: Exploring cognitive biases in large language models through Multi-Agent Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2410.04452?

35.A Tutorial on Cognitive Biases in Agentic AI-Driven 6G Autonomous Networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2510.19973 36.Can A Society of Generative Agents Simulate Human Behavior and Inform Public Health Policy? A Case Study on Vaccine Hesitancy | OpenReview, erişim tarihi Haziran 3, 2026, https://openreview.net/forum?id=zSbecER9il 37.Can A Society of Generative Agents Simulate Human Behavior and Inform Public Health Policy? — A Case Study on Vaccine Hesitancy - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2503.09639v4 38.Can A Society of Generative Agents Simulate Human Behavior and Inform Public Health Policy? A Case Study on Vaccine Hesitancy - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2503.09639v2 39.GitHub - abehou/VacSim: The official repository for paper: Can A Society of Generative Agents Simulate Human Behavior and Inform

Public Health Policy? A Case Study on Vaccine Hesitancy, erişim tarihi Haziran 3, 2026, https://github.com/abehou/VacSim 40.Simulating Misinformation Vulnerabilities With Agent Personas - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2511.04697v1 41.Simulating Misinformation Diffusion on Social Media Through CoNVaI: A Textual- and Agent-Based Diffusion Model - IJCAI, erişim tarihi Haziran 3, 2026, https://www.ijcai.org/proceedings/2025/0029.pdf

42.Artificial Intelligence, Deepfakes, and Disinformation: A Primer - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1000/PEA1043-1/RAND_PEA1043-1.pdf 43.Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept - Frontiers, erişim tarihi Haziran 3, 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/ full 44.Crossing the Deepfake Rubicon - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/crossing-deepfake-rubicon 45.Foreign Malign Influence Targeting U.S. and Allied Corporations - CSIS, erişim tarihi

Haziran 3, 2026,

https://www.csis.org/analysis/foreign-malign-influence-targeting-us-and-allied-corporations 46.Impacts of Adversarial Use of Generative AI on Homeland Security, erişim tarihi Haziran 3, 2026, https://www.dhs.gov/sites/default/files/2025-01/25_0110_st_impacts_of_adversari al_generative_aI_on_homeland_security_0.pdf 47.Cognitive Warfare - Belfer Center, erişim tarihi Haziran 3, 2026, https://www.belfercenter.org/sites/default/files/pantheon_files/2019-11/Cognitive Warfare.pdf 48.[2304.03442] Generative Agents: Interactive Simulacra of Human Behavior - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2304.03442 49.Cognitive Warfare Is Exploiting Polarization, Both in Nations and Companies, erişim tarihi Haziran 3, 2026, https://www.asisonline.org/security-management-magazine/articles/2026/04/cognitive-warfare/ 50.Cognitive Warfare | NATO Science and Technology Organization, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/document/cognitive-warfare/ 51.How to Lose an Information War in 10 Days - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/how-lose-information-war-10-days

52.The Cognitive Battlefield of Hybrid Warfare - Nato Defense College Foundation, erişim tarihi Haziran 3, 2026, https://www.natofoundation.org/food/the-cognitive-battlefield-of-hybrid-warfar e/ Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz;

Bu bölümün geniş okuması yapılırken davranışsal modelleme yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası sınırlı rasyonellik, bilişsel önyargı, ajan tabanlı simülasyon ve sentetik nüfus üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle davranışsal modelleme alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma

yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● ● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Davranışsal Modelleme ve Ajan Tabanlı Simülasyonlar alanında en güçlü erken uyarı
göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

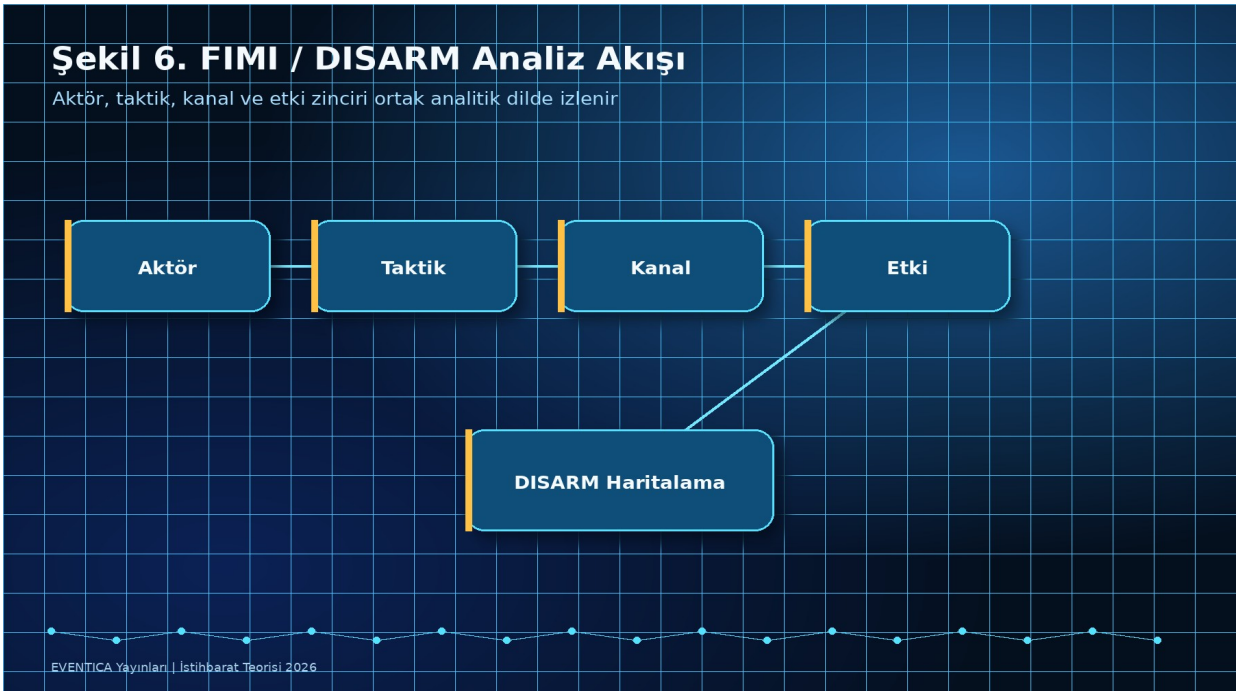
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 6. Siber-Bilişsel Kesişimde FIMI ve DISARM Çerçevesi

FIMI, dezenformasyonun sadece içerik değil; aktör, davranış, kanal, hedef ve etki zinciri olarak okunması gerektiğini gösterir.



Şekil 6. FIMI/DISARM analizinde saldırı ve savunma döngüsü

Tablo 9. FIMI analiz katmanları

Katman	Soru	Savunma çıktısı
Aktör	Kim yönlendiriyor veya destekliyor?	Atıf değerlendirmesi
Davranış	Koordinasyon var mı?	Operasyon örüntüsü
İçerik	Hangi anlatı taşınıyor?	Anlatı haritası
Kanal	Hangi ağlarda yayılıyor?	Dağıtım zinciri
Etki	Hangi karar veya güven alanı hedefleniyor?	Risk ve yanıt planı

Siber-Bilişsel Kesişimde Dış Bilgi Manipülasyonu (FIMI): Dezenformasyon Analiz ve Risk Yönetimi (DISARM) Çerçevesi Kavramsal Çerçeve: Bilişsel Harp, FIMI ve Hibrit Tehditler Ekseninde Stratejik Yeniden Konumlandırma Geleneksel bilgi güvenliği paradigması ve kinetik savaş doktrinleri, yirmi birinci yüzyılın ikinci çeyreğine girerken köklü bir yapısal dönüşüm geçirmiştir. Bu dönüşümün merkez üssü, teknolojik altyapılar ile insan zihninin doğrudan birbirine bağlandığı, etkileşime girdiği ve birbirini manipüle ettiği "siber-bilişsel kesişim" (cyber-cognitive intersection) alanıdır.1 Modern çatışma ortamı, artık yalnızca fiziksel toprakların veya dijital ağların ele geçirilmesiyle değil, toplumların anlamlandırma kapasitelerinin, ortak yargı alışkanlıklarının ve karar alma mekanizmalarının doğrudan kontrol edilmesiyle tanımlanmaktadır. Bu stratejik

ortamı analitik bir zeminde anlamlandırabilmek için, sıklıkla birbirinin yerine kullanılan ancak operasyonel hedefleri, analiz seviyeleri ve teorik temelleri bakımından farklılık gösteren üç temel kavramın sınırlarının kesin hatlarla çizilmesi gerekmektedir: Bilişsel Harp (Cognitive Warfare), Dış Bilgi Manipülasyonu ve Müdahalesi (FIMI) ve Hibrit Tehditler (Hybrid Threats).1 Bilişsel Harp, düşmanın algılarını, inançlarını ve karar alma süreçlerini manipüle ederek stratejik ve asimetrik avantaj elde etmeyi amaçlayan, teknolojinin, sinirbilimin ve insan bilişinin eşgüdümlü bir şekilde silahlaştırılmasıdır.1 NATO ve askeri literatür bağlamında bilişsel harp, bilgi operasyonlarının yalnızca bir alt kümesi veya destekleyici bir unsuru olmaktan çıkmış, operasyonların birincil ekseni (primary line of operations) haline gelmiştir.6 Askeri düşünürler ve stratejistler (örneğin Claverie ve du Cluzel) bilişsel harpı, insan beynini modern savaşın altıncı alanı olarak konumlandırarak açıklamaktadır.4 Bu yaklaşım, bilginin kendisini bir amaç olarak değil, insan bilişini hacklemek için kullanılan bir araç olarak görür.

Öte yandan, Avrupa Birliği Dış İlişkiler Servisi (EEAS) tarafından uluslararası güvenlik lügatine kazandırılan Dış Bilgi Manipülasyonu ve Müdahalesi (FIMI) kavramı, devlet veya devlet destekli dış aktörlerin, hedef toplumların demokratik prosedürlerini, politikalarını ve değer yargılarını bozmak amacıyla yürüttükleri koordineli ve kasıtlı dezenformasyon faaliyetlerini kapsar.8 Kanada Güvenlik İstihbarat Servisi (CSIS) ve Japonya'daki stratejik değerlendirmeler de FIMI'yi doğrudan bir ulusal güvenlik tehdidi olarak tanımlamakta ve demokrasilerin bu tür manipülasyonlara karşı korunmasının, tehdit aktörleriyle yüzleşmeyi gerektirdiğini vurgulamaktadır.12 FIMI, bilişsel harpın sivil, politik ve diplomatik arenadaki yansımasıdır; asıl hedefi doğrudan askeri karar alma döngüleri değil, sivil toplumun kurumsal direncidir.

Hibrit Tehditler ise, devlet ve devlet dışı aktörlerin eşzamanlı, çok boyutlu ve esnek saldırılarını ifade eder. Hibrit savaş, diplomatik, askeri, ekonomik ve teknolojik araçların

konvansiyonel savaş eşiğinin altında harmanlanmasıyla kurumların ve uluslararası düzenin direncini test eder.1 bilişsel harp ve FIMI, hibrit tehditlerin bilgi uzayındaki alt bileşenleri olarak işlev görse de, hibrit tehditlerin kapsamı fiziksel sabotajlardan ekonomik ambargolara kadar uzanan daha geniş bir yelpazeye yayılır.

Giovanni Sartori'nin "kavramsal esneme" (conceptual stretching) teorisi bağlamında bakıldığında, mevcut kurumların farklı fenomenleri kapsamak için kavramları kendi çıkarlarına veya analitik ihtiyaçlarına göre esnetmesi, disiplinler arası bir iletişim kopukluğuna neden olmaktadır.1 Bu kavramsal asimetriyi gidermek, etkili bir savunma inşa etmenin ön koşuludur.

Aşağıdaki tablo, bu üç stratejik kavramın temel boyutlarını, analiz seviyelerini ve değerlendirme kriterlerini karşılaştırmalı olarak sunmaktadır:

Boyut Analiz Seviyesi (Level of Temel Hedefler ve Analysis) Değerlendirme Kriterleri Bilişsel Harp (Cognitive Birey, askeri birim, Karar kalitesi, tempo, güven Warfare) organizasyon, kurum veya kalibrasyonu ve baskı genel nüfus (Etkiler altında davranışın seviyeler arası yayılabilir). manipülasyonu.3 FIMI / Etki Faaliyetleri Temel olarak genel nüfus, Meşruiyet erozyonu, sivil toplum, diaspora demokratik süreçlerin toplulukları veya karar verici bozulması, erişim/etkileşim politik elitler.

metrikleri.5 Hibrit Tehditler Sivil toplumun tamamı, kritik Senkronize eylemlerin altyapılar ve uluslararası yarattığı çok alanlı krizler ve yasal/ekonomik düzen. kurumsal felç hali.3 Karar odaklı bu yeni tehdit ekosisteminde, "Bilişsel Savunma" (Cognitive Defense) kavramı kritik bir doktriner ağırlık kazanmıştır. Bilişsel savunma, basit bir yalanlama veya karşı-mesajlaşma (counter-messaging) reaksiyonu değildir. İnsan zihnini düşmanın algı mühendisliğinden koruyan, asimetrik tehdit altında dahi karar alma kapasitesini sürdürülebilir kılan operasyonel bir mimaridir.5 Bu savunma konsepti, bilişsel alanda tehdit tespiti, algısal dayanıklılık, sürekli adaptasyon ve kurumsal öğrenme süreçlerini bütünleşik bir şekilde işletmeyi zorunlu kılar.18

Akademik Teoriler: Bilişsel Etkileşim Metrikleri ve Karar Döngüsü Dinamikleri bilişsel harp

ve FIMI operasyonlarını ampirik bir düzleme taşımak, modern askeri ve akademik literatürün en büyük zorluklarından biri olmuştur. Geleneksel siber güvenlik, paket kayıplarını, yetkisiz erişimleri veya sızdırılan veri boyutunu baytlar cinsinden ölçebilirken; bilişsel harp, korku, kutuplaşma, şüphe ve inanç erozyonu gibi soyut fenomenler üzerinden ilerler. Bu soyutluğu somut veri setlerine dönüştüren akademik teoriler, operasyonel savunmanın bel kemiğini oluşturur.

Bu teorik inşaların başında, bilişsel saldırıların "Etkileşim Verimliliğini" (Engagement Effectiveness) matematiksel bir modelle ölçmeyi amaçlayan ampirik çalışmalar gelmektedir.

Bonnie Rushing ve Shouhuai Xu (2025) tarafından literatüre kazandırılan çerçeve, asimetrik bilişsel saldırıların sosyal medya platformlarındaki davranışsal etkisini nicel olarak hesaplayan devrimsel bir metrik sunmuştur.19 Bu modele göre, FIMI operasyonlarının başarısı yalnızca

içerik üretimine değil, üretilen içeriğin hedef kitleyle ne derece yoğun bir psikolojik etkileşime girdiğine bağlıdır. Model, etkileşim verimliliğini savunma ve risk analizi amacıyla şu soyut formülle ifade eder:

$$\mathbf{EV = (\Sigma_i w_i \times r_i) / C}$$

Bu denklemde EV, Etkileşim Verimliliğini (Engagement Effectiveness) temsil eder. r_i, kullanıcı tepkilerini; w_i, bu tepkilerin göreli ağırlığını; C ise içeriğin üretim, yayılım ve operasyonel maliyetini gösterir. Örneğin görüntüleme, beğenme, yorum, paylaşım ve kaydetme gibi davranışlar aynı ağırlıkta değerlendirilmez; karar verici için daha yüksek etki doğuran davranışlara daha yüksek katsayı verilir.

Bu modelin stratejik okuması şudur: düşük maliyetli ve sınırlı hacimli bir içerik akışı, hedef kitlede yüksek düzeyde tepki, kutuplaşma, güven erozyonu veya karar sapması oluşturuyorsa etkileşim verimliliği yükselir. Bu nedenle metrik, manipülatif kampanyaları büyütmek için değil; FIMI operasyonlarının davranışsal etkisini erken tespit etmek, savunma önceliği üretmek ve karşı dayanıklılık stratejilerini ölçmek için kullanılmalıdır. Bilişsel müdahalenin zaman içindeki evrimini ve hedef üzerindeki tahribatını açıklayan ikinci kritik akademik teori, Birleşik Devletler Hava Kuvvetleri'nden Albay John Boyd tarafından geliştirilen ve bilişsel harpa uyarlanan Gözlemle-Yönel-Karar Ver-Uygula (OODA) döngüsüdür.5 bilişsel harp literatürü, FIMI'yi hedef kitlenin OODA döngüsünü bozmaya, geciktirmeye veya tamamen çarpıtmaya yönelik bir mücadele olarak tanımlar.17 Bu yaklaşıma göre başarı, anlatıların kaç kişiye ulaştığıyla değil; bilişsel etkilerin zaman içinde hedef kitlenin yargı yetisini ne kadar bozduğu, eylemlerini nasıl değiştirdiği ve güveni nasıl yok ettiğiyle ölçülür.

Frontiers in Big Data dergisinde yayımlanan araştırmaların da teyit ettiği üzere, yapay zekâ destekli bilişsel harp taktikleri, toplumların "anlamlandırma" (sense-making) kapasitelerini hedef alır.21 Bu taktikler, insan bilişinin doğal zayıflıkları olan sezgisel düşünme eğilimlerini (heuristics), bilişsel önyargıları (cognitive biases) ve duygusal reaksiyonları sömürür. Hazırlama (priming), dürtme (nudging), zamanlama (timing) ve aldatma (deception) gibi psikolojik teknikler kullanılarak karar alma döngüleri felç edilir.22 OODA döngüsünün 'Karar Ver' (Decide) ve 'Uygula' (Act) aşamalarında Saldırganın (Attacker) yarattığı etkiler ile Savunmacının (Defender) geliştirdiği koruma mekanizmaları arasındaki akademik ayrım, aşağıdaki tabloda özetlenmiştir:

OODA Aşaması Saldırgan Etki Kategorisi Savunmacı Etki Kategorisi (Attacker Effects)

(Defender Effects)

Karar Ver (Decide) Karar Etkileri: Hedef Karar Koruması: Bilişsel kitlenin yargı yetisini bozan stres ve belirsizlik altında bilişsel kısayollara bağımlılığı karar kalitesini, karar alma artırmak, aşırı güven, şüphe temposunu ve kurumsal veya kafa karışıklığı güveni muhafaza etmek.5 yaratmak.5 Uygula (Act) Eylem Etkileri: Hedefi Eylem Koruması: erken eyleme geçmeye, Operasyonel niyetin yanlış odaklı tepkiler bütünlüğünü korumak; vermeye veya kasıtlı saldırgan kaynaklı hatalı eylemsizliğe (non-action) eylemleri veya eylemsizliği sürükleyerek saldırgana önleyerek görev amacını fayda sağlamak.5 güvence altına almak.5 Bu akademik teoriler, FIMI eylemlerinin salt bir halkla ilişkiler krizi veya ifade özgürlüğü sınırlarında değerlendirilebilecek basit bir "yanlış bilgi" sorunu olmadığını kanıtlamaktadır. Bilgi uzayının matematiksel ve psikolojik parametrelerle ölçülebilen ve OODA döngüsü üzerinden simüle edilebilen bir silah (weaponized information) halini alması 14, mevcut savunma mimarilerinin de bu bilimsel gerçekliğe uygun olarak yeniden tasarlanmasını zorunlu kılmıştır.

Sistem Mimarisi: DISARM Çerçevesinin (Dezenformasyon Analiz ve Risk Yönetimi) Ontolojisi Modern bilişsel operasyonların sarmal yapısı, savunma aktörlerinin ortak bir dilde iletişim kurmasını ve istihbarat paylaşmasını kaçınılmaz hale getirmiştir. Tehditlerin "siber-bilişsel" kesişimde gerçekleşmesi, siber güvenlik dünyasının yıllar içinde olgunlaştırdığı metodolojilerin bilgi uzayına aktarılmasını gerektirmiştir. Bu ihtiyacın stratejik çıktısı, Dezenformasyon Analiz ve Risk Yönetimi (DISARM) Çerçevesi'dir.23 Çerçevenin Tarihsel Evrimi ve Felsefesi DISARM, siber güvenlik endüstrisinde bir endüstri standardı olan MITRE ATT&CK matrisinin tasarım felsefesini örnek alarak oluşturulmuş, bilgi operasyonlarını ad hoc etiketleme süreçlerinden kurtarıp yapılandırılmış, makine tarafından okunabilir (machine-readable) bir taksonomiye dönüştüren açık kaynaklı ana mimaridir.25 Çerçevenin kökleri, 2018 yazında uluslararası bir hibrit savaş çalıştayında bir araya gelen stratejistlerin vizyonuna dayanır.27 2019 yılında Craig Newmark Philanthropies'in desteğiyle, MisinfoSec Standartları Çalışma Grubu ve Credibility Coalition altında "AMITT" (Adversarial Misinformation Influence Tactics & Techniques) adıyla yapılandırılmıştır.27 AMITT, Birleşmiş Milletler, Dünya Sağlık Örgütü, Avrupa Birliği ve NATO gibi devasa organizasyonların dezenformasyon krizlerinde (örneğin COVID-19 pandemisi sırasındaki CTI League faaliyetlerinde) kullanılmaya başlanmasıyla

rüştünü ispat etmiştir.26 MITRE Corporation ile kurulan doğrudan temaslar neticesinde AMITT, STIX (Structured Threat Information Expression) ve MISP standartlarıyla uyumlu hale getirilmiştir.27 Çerçevenin gelişimi, 2021 yılının sonlarında "DISARM Vakfı"nın (Birleşik Krallık merkezli bir Toplumsal Çıkar Şirketi - C.I.C.) kurulması ve isminin resmi olarak DISARM olarak güncellenmesiyle kurumsallaşmıştır.23 Vakıf, çerçeveyi CC-BY-SA-4.0 lisansı altında topluluğa ait, sürekli güncellenen ve açık kaynaklı bir "ağların ağı" (network of networks) mimarisi olarak korumaktadır.2 Alliance4Europe, Alfred Landecker Vakfı ve Public Democracy gibi kuruluşların desteklediği bu yapı, günümüzde FIMI olaylarını analiz etmek için "Mendeleyev'in Bilgi Operasyonları Tablosu" olarak adlandırılmaktadır.27 DISARM sistem mimarisi, ontolojik olarak birbirine entegre iki ana operasyonel modelden oluşur:

Saldırganın niyet ve eylemlerini kategorize eden Kırmızı Çerçeve (Red Framework) ve savunmacının müdahale seçeneklerini listeleyen Mavi Çerçeve (Blue Framework).28 Kırmızı

Takım Çerçevesi (Red Framework): Saldırı Vektörlerinin Kodlanması

Kırmızı Çerçeve, bilgi manipülasyonu oluşturan devlet ve devlet dışı aktörlerin TTP'lerini (Taktikler, Teknikler ve Prosedürler) bir dezenformasyon operasyonunun yaşam döngüsüne (kill chain) uygun olarak dört ana evrede sınıflandırır.30 Bu yapılandırma, tehdit analizcilerine düşmanın stratejik zihnine girme (Adopt the attacker's lens) imkanı sunar 32:

1. Planlama (Plan): Operasyonun zihinsel ve stratejik temelinin atıldığı evredir. Saldırgan,

hedef aldığı kitlenin psikolojik fay hatlarını inceler. Stratejik sonların belirlenmesi (T0074: Determine Strategic Ends), hedef kitlenin zayıf noktalarının tespit edilmesi (T0073:

Determine Target Audiences) ve mevcut istihbarat verilerinin işlenmesi bu aşamada gerçekleşir.31 Bu, operasyonun navigasyon sisteminin kurulduğu fazdır.

2. Hazırlık (Prepare): Planlanan operasyonun dijital ve sosyal altyapısının inşa edildiği

aşamadır. FIMI aktörleri, inandırıcı görünmek için "Potemkin köyleri" kurarlar. Özgün olmayan (inauthentic) sosyal medya hesaplarının, sayfaların ve grupların oluşturulması (T0007), sahte haber sitelerinin yayına alınması (T0013) ve bilgisiz aracıların (kullanışlı aptallar - ignorant agents) ağa dahil edilmesi (T0010) bu sürecin omurgasıdır.34 Saldırgan ayrıca mevcut anlatıları kullanma (T0003), komplo teorilerinden yararlanma (T0022) ve rakip anlatılar geliştirme (T0004) yoluyla içerik üretir.34

3. Uygulama (Execute): Hazırlanan manipülatif içeriğin siber ve sosyal kanallar aracılığıyla

bilgi uzayına enjekte edildiği ve maksimize edildiği aşamadır.35 Bu faz, bilginin aktif olarak

silahlaştığı noktadır. Düşmanı küçültme ve itibarını zedeleme (T0066), devlet propagandasını kolaylaştırma (T0002) veya gerçeği reddetme (T0075) gibi taktikler uygulanır.34 Özellikle bot ağlarıyla gerçekleştirilen "bilgi uzayını sel baskınına uğratma" (Flooding - T0049), algoritmik manipülasyon için kilit olan "Pompa Hazırlama" (Conduct Pump Priming) ve operasyonun finansmanı için sahte kitle fonlamaları düzenleme (T0017) eylemleri bu aşamada koordine edilir.34 Failler kimliklerini gizler (T0128) ve uzun vadeli bir yıpratma savaşı yürütür (T0059).34

4. Değerlendirme (Assess): Başlatılan kampanyanın etkinliğinin, hedeflenen metrikler

(etkileşim, toplumsal kutuplaşma vb.) üzerinden değerlendirildiği son aşamadır (T012: Assess Effectiveness).31 Bu geri bildirim döngüsü, saldırganın OODA döngüsünü tamamlayarak bir sonraki operasyonun planlama fazına veri sağlar.

Mavi Takım Çerçevesi (Blue Framework): Savunma ve Azaltım Spektrumu Siber güvenlik olay müdahale (incident response) mantığını temel alan Mavi Çerçeve, Kırmızı Çerçevede tanımlanan düşman taktiklerine karşı uygulanabilecek "karşı önlemler" (countermeasures) dizisidir.30 Mavi çerçeve, tespit edilen TTP'ler ile doğrudan bir haritalandırma (direct mapping) sunarak kriz anında karar vericilerin çevik (agile) adımlar atmasını sağlar.37 Bu tepki modeli, sadece içeriğin çürütülmesini değil, operasyonun tüm finansal ve algoritmik bacaklarının kesilmesini de içerir.

Öne çıkan Mavi Takım azaltım (mitigation) mekanizmaları şunlardır 34:

- ● Bilişsel Aşılama ve Çürütme: Hedef kitleyi manipülatif anlatılarla karşılaşmadan önce

bağışıklık kazandıran "Önceden Çürütme" (Prebunking - C00125), sahte uzmanların veya itibar mühendisliği ürünlerinin maskesini düşürme (Debunk and defuse a fake expert/credentials - C00113) ve gerçeğe dayalı ikna edici karşı anlatılar geliştirme (C00030).

- ● Algoritmik ve Finansal Kesinti: Dezenformasyon içeriklerinin yayılmasını yavaşlatmak için

arama algoritmalarının değiştirilmesi (Change search algorithms - C00078), şikayet edilen hesapların platformlardan hızla kaldırılmasının sağlanması (C00189) ve kötü niyetli aktörlerin para akışını kesmek için bankacılık ağlarına erişiminin durdurulması (Use banking to cut off access - C00129) ile reklamveren kontrollerinin kullanılması (C00216).

- ● Altyapısal Hedefleme: Açık kaynak istihbaratını (OSINT) kullanarak "Potemkin köylerini"

açığa çıkarma (Unravel the Potemkin villages - C00162) ve kar amacı güden etkileşim fabrikalarına (engagement factories) karşı yasal işlem başlatma (C00060).

Ancak Mavi Çerçeve, içerisinde demokratik değerlerle örtüşmeyebilecek radikal önlemler de barındırır. Örneğin, açık kaynaklı gönüllü atölyelerinde belirlenen bazı karşı önlemler

"Sansür"

(Censorship - C00016) taktiğini içermektedir.30 DISARM Vakfı, otokratik eğilimli ülkelerde gözlemlenen bu tür taktiklerin kullanımı konusunda kullanıcıları açıkça uyararak; savunma eylemlerinin orantılı, etik ve demokratik normatif sınırlara uygun olması gerektiğini vurgulayan "Refakatçi Kılavuzlar" (Companion Guides) yayımlamıştır.30 Teknolojik Bütünleşme ve İstihbarat Platformları (TIP) DISARM'ın gerçek gücü statik bir matris olmasından değil, modern siber tehdit istihbaratı mimarilerine entegre edilebilmesinden gelir. DISARM verileri, STIX 2.1 (Structured Threat Information Expression) ve TAXII gibi açık standart şablonları üzerinden ISAOs (Bilgi Paylaşımı ve Analiz Organizasyonları) arasında kolayca paylaşılabilecek formatta tasarlanmıştır.25 EclecticIQ gibi kurumsal Tehdit İstihbarat Platformlarına (TIP) entegrasyon sağlandığında, DISARM verileri ad hoc bir Excel tablosu olmaktan çıkar.25 EIQ-JSON gibi standartlarda dışa aktarılabilen TTP'ler, interaktif görsel kontrol panelleri, ağ grafikleri (network graphs) ve ısı haritaları (heatmaps) üzerinden görselleştirilir.25 Bu görselleştirme, yüzlerce farklı kampanya arasında paylaşılan davranışsal imzaları (behavioral signatures) ve FIMI aktörlerinin zaman içindeki taktiksel evrimini otomatik

olarak haritalandırarak siber analistlere eşsiz bir ortak durumsal farkındalık (situational awareness) sağlar.25 Gerçek Dünya Vakaları: Teoriden Pratiğe FIMI Operasyonları DISARM çerçevesinin teorik inşası ve ampirik metriklerin geçerliliği, ancak spesifik jeopolitik kriz vakalarına uygulandığında tam anlamıyla kavranabilir. Dünya genelindeki bilişsel saldırılar, FIMI aktörlerinin ne denli sofistike ve çok alanlı hareket ettiğini ortaya koymaktadır.

Vaka 1: 2025 Moldova Seçimleri ve Çok Ajanlı Otonom Ağ Keşfi bilişsel harp mekanizmalarının ve otonom analizin sahada test edildiği en güncel ve çarpıcı örneklerden biri, 2025 Moldova Seçimleridir.41 Seçimlere dış müdahale bağlamında, Moldova bağlantılı Telegram kanallarını hedefleyen devasa bir operasyon yürütülmüştür.42 Otonom yapay zekâ ajanlarının DISARM çerçevesiyle entegre edilerek yürütüldüğü araştırmada, toplam

595.814 yorumdan oluşan devasa bir veri seti analiz edilmiştir.42 İnsan analistlerin veya eski nesil kural tabanlı sistemlerin yürüttüğü önceki analizlerde gözden kaçan detaylar, yapay zekâ ajanları sayesinde gün yüzüne çıkarılmıştır. Otonom sistem, toplam 584 bot hesabı tespit etmiş ve bu botların seçim döneminde 86.448 adet koordineli politik yorum ürettiğini belgelemiştir.42 Daha da önemlisi, ajan destekli sistem, daha önceki manuel incelemelerde tespit edilemeyen, stratejik olarak uyutulmuş 30'dan fazla Rus bağlantılı bot hesabını yüzeye çıkarmıştır.41 Bu operasyon, DISARM'ın Kırmızı Çerçevesindeki "Bilgi Uzayını Sel Baskınına Uğratma" (T0049: Flooding the information space) taktiğinin ders kitabı niteliğinde bir uygulamasıdır.38 Ajan mimarisi, hedef kitlenin politik kararlarını etkilemek için yaratılan bu algoritmik gürültüyü makine hızında çözümleyerek, otonom savunmanın zaruretini ispat etmiştir.

Vaka 2: 2016 ABD Seçimleri ve Mendeleyev Tablosunun Doğuşu Rusya merkezli İnternet Araştırma Ajansı'nın (IRA), 2016 Amerika Birleşik Devletleri Başkanlık Seçimleri'ne yönelik operasyonu, modern FIMI'nin sıfır noktası olarak kabul edilir.29 ISSP analizlerine göre bu operasyon, DISARM Çerçevesinin bir "Mendeleyev'in Bilgi

Operasyonları

Tablosu" gibi okunmasına olanak tanıyan kusursuz bir "Kırmızı Takım" örneğidir.29 IRA, Planlama aşamasında ABD toplumundaki ırksal, ekonomik ve politik kırılma hatlarını tespit etmiş; Hazırlık aşamasında binlerce sahte sosyal medya personası, sivil toplum grubu görünümünde sayfalar yaratmış; Uygulama aşamasında ise bu sahte profiller üzerinden hedeflenmiş politik reklamlar (microtargeting) vererek seçmen davranışını doğrudan manipüle etmiştir.29 2016 operasyonunun yarattığı kurumsal şok, Batı demokrasilerinde siber ve bilişsel politikaların birleşmesine ve DISARM gibi defansif (Mavi Takım) mimarilerin geliştirilmesine ön ayak olmuştur.

Vaka 3: Savaş Alanında Sentetik Medya ve Algı Manipülasyonu Bilgi ortamının fiziksel bir savaş alanını doğrudan şekillendirdiği asimetrik örnekler, Rusya-Ukrayna ve İsrail-Hamas çatışmalarında açıkça görülmüştür.43 Savaşın ilk safhalarında ortaya çıkan ve Ukrayna Devlet Başkanı Vladimir Zelenskiy'i ordusuna teslim olma çağrısı yaparken gösteren Rus menşeli "deepfake" (derin sahtekarlık) videosu, bilişsel harpın şahikasıdır.7 Bu olay, DISARM çerçevesindeki rakip anlatılar geliştirme (T0004), düşmanı küçültme (T0066) ve gerçeği inkar etme (T0075) taktiklerinin sentetik medya kullanılarak uygulanmasıdır.34 Benzer şekilde, IŞİD veya Wagner Grubu gibi asimetrik devlet dışı

aktörlerin, işledikleri vahşet suçlarını sosyal ağlar üzerinden glorifiye ederek kitlelerde terör ve psikolojik felç yaratma çabaları, bilgi operasyonlarını destekleyici bir unsur olmaktan çıkarıp, doğrudan bir birincil operasyon hattına taşımıştır.7 Vaka 4: Avrupa'nın Enerji Dönüşümünde

Kurumsal Etki Operasyonları

bilişsel harp sadece devletler arası jeopolitik krizlerde değil, küresel politikaları etkilemeye çalışan devasa kurumsal etki operasyonlarında da görülmektedir.44 Avrupa'nın yenilenebilir enerjiye geçiş ve iklim hedeflerine yönelik süreçlerde, devlet

destekli veya kurumsal çıkarlara dayanan FIMI aktörleri, yeşil enerji politikalarının maliyetleri veya güvenilirlikleri üzerine sahte veriler üreterek politikaları sekteye uğratmayı amaçlamıştır. Bu süreç, anlatı akışlarını haritalandıran araçların ve "deepfake" tespit mekanizmalarının politika uygulamalarında hala ne kadar az gelişmiş olduğunu gözler önüne sermiş ve Avrupa Birliği'ni kurumsal bilişsel esnekliği (cognitive resilience) güçlendirecek stratejiler aramaya itmiştir.44

Mekanizma Analizi: Yapay Zekâ Tabanlı (Agentic) İşletim Modeli Yukarıda incelenen devasa

sosyal ağ verileri ve sofistike botnetler, insan analistlere dayalı geleneksel ve manuel DISARM etiketleme süreçlerinin artık siber hızda (machine speed) yetersiz kaldığını göstermektedir.8 FIMI kampanyaları yapay zekâ ile otomatikleştirilirken, savunmanın insan hızında kalması stratejik bir zafiyettir. Bu zafiyeti aşmak için Tseng ve diğerleri (2026) tarafından literatüre kazandırılan "Ajanlı İşletim Modeli" (Agentic Operationalization), DISARM mimarisini Otonom Yapay Zekâ ile birleştiren bir mekanizmadır.8 Bu sistem, FIMI tespitini Komuta, Kontrol, İstihbarat, Gözetleme ve Keşif (C2ISR) süreçlerine otonom olarak entegre eder.8 Mekanizmanın çekirdeği, BMAD-METHOD (Çevik Yapay Zekâ Odaklı Geliştirme İçin Çığır Açıcı Yöntem) üzerine inşa edilmiş çoklu ajan (multi-agent) işlem hattıdır (pipeline).10 Ajanlar arası etkileşim, sürekli bir döngü içerisinde hipotez üreten ve test eden şu aşamalardan oluşur:

1. Keşfedici Veri Analizi (Exploratory Data Analysis - EDA): Yapay zekâ ajanı, ilk turda SQL

gibi veritabanlarından elde edilen ham sosyal medya verilerini tarar. Ajan bu aşamada herhangi bir anomali veya manipülasyon tespiti yapmaya çalışmaz; yalnızca veri setinin istatistiksel sınırlarını, zaman aralıklarını, toplam yorum sayısını ve platforma özgü metadata özelliklerini haritalandırır.38 Bu gecikmeli yaklaşım (deferred approach), daha sonra bulunacak anormalliklerin genel hatalar yerine spesifik DISARM tekniklerine atfedilmesini güvence altına alır.38

2. TTP Örneklemesi ve Çok Kollu Haydut (Multi-Armed Bandit) Stratejisi: Klasik istatistiksel

algoritmalar yerine, ajanlar Büyük Dil Modelleri (LLM) tarafından yönlendirilen bir

"Keşfet-Sömür" (Explore-Exploit) taktiği uygular.10 ○ Keşfet Modu (İlk İterasyonlar): Ajan, DISARM taksonomisinin tüm dallarını kapsayabilmek için daha önce veri setinde hiç test edilmemiş Kırmızı TTP'leri (örneğin T0073 veya T0010) rastgele seçerek analiz eder.

○ Sömür Modu (İlerleyen İterasyonlar): Eğer ajan belirli bir taktiğe dair (örneğin bot hesaplarla bilgi alanını doldurmayı ifade eden T0049) güçlü sinyaller alırsa, sistem bu bulguyu derinleştirmek için o tekniği sömürmeye başlar. Keşif-Sömür dengesi, başarısız denemelerden sonra keşfe, güçlü sinyallerden sonra sömürüye doğru dinamik olarak uyarlanır.10

3. Alt Süreç Aktarımları (Subprocess Relays) ve Bulgu İlişkilendirmesi: Ajanlar, 15 ayrı

inceleme turu boyunca birbirlerine veri aktarımı yaparak tutarlı bir yürütme sağlar. Bulunan her bir manipülatif davranış kalıbı, spesifik bir DISARM tekniğine (ID) etiketlenir ve bulgu ile TTP arasındaki şeffaf bağlantı korunur.38

4. Atomik Kanıt Parçalanması ve İstatistiksel Doğrulama (Atomic Evidence Decomposition):

Yapay zekâ destekli savunma sistemlerinin en büyük zayıflığı olan "halüsinasyon" (LLM'lerin sahte veri üretmesi) problemini çözmek için devrimsel bir yöntem kullanılır. Karmaşık istihbarat bulguları, ayrık ve doğrulanabilir "atomik" alt iddialara bölünür. Her

bir iddia, istatistiksel doğrulama üzerinden geçer/kalır kriterlerine (pass/fail criteria) tabi tutulur.38 Böylece LLM tarafından üretilen kanıtların tekrarlanabilirliği ve güvenilirliği matematiksel olarak kanıtlanmış olur.

Bu "teknik güdümlü ajan mimarisi" (technique-guided agent architecture), OODA döngüsünün Gözlem ve Yönelme (Observe-Orient) aşamalarını saniyelere sıkıştırarak analist kapasitesini çarpan etkisiyle artırır.8 DISARM, bu otonom makinenin ürettiği verilerin insan analistler tarafından hala "yorumlanabilir" ve operasyonel doktrine uygun kalmasını sağlayan yegane anlamsal omurgadır (semantic backbone).8

Trend Analizi (2020–2026): Bilişsel Harpın Radikal Evrimi

Stratejik çevre, 2020 ile 2026 yılları arasında FIMI tehditlerinin doğası, araçları ve savunma doktrinleri bağlamında geri döndürülemez bir paradigma kayması yaşamıştır. bilişsel harpı şekillendiren temel trendler şu eksenlerde incelenebilir:

1. Üretken Yapay Zekânın (Generative AI) Manipülasyonu Demokratikleştirmesi: 2020

öncesinde sosyal medya manipülasyonları ağırlıklı olarak düşük profilli bot ağlarına, kopyala-yapıştır mesajlarına ve fiziksel "troll fabrikalarına" dayanırken, Üretken Yapay Zekâ teknolojilerinin (LLM'ler, görsel üreteçler) gelişimi tabloyu tamamen değiştirmiştir.7

Günümüzde FIMI, sentetik medyanın (deepfakes), sarmalayıcı ortamların (immersive environments) ve kişiselleştirilmiş anlatıların otomasyonu üzerinden ilerlemektedir.45 Özellikle 2026 itibarıyla RAND araştırmacılarının dikkat çektiği "anlatı dilinin oyunlaştırılması" (gamification of narrative language), devlet destekli aktörlerin hedef kitlenin alt-kültür argosunu, oyuncu terminolojisini ve internet mimlerini (memes) kusursuzca taklit etmesini sağlamıştır.46 Bu gelişme, ABD ve müttefikleri için yeni çatışmaların füzelerden önce "oyuncu argosu ve aşağılayıcı anlatılarla" başlayacağına işaret etmektedir.46

2. Bilişsel Harpın Algıdan "Anlamlandırma Mimarisine" Yönelmesi: Estonya'nın başkenti

Tallinn'deki NATO Mükemmeliyet Merkezi (CCDCOE) tarafından 2026'da yayımlanan "Invisible by design" (Tasarım Gereği Görünmez) başlıklı rapor, tehdit vektörünün yön değiştirdiğini kanıtlamaktadır.47 Analizler, bilişsel saldırıların artık yalnızca spesifik yalan haberler veya deepfake propagandası yaymaktan ibaret olmadığını ortaya koymaktadır. Asıl hedef, kurumların ve toplumların "dünyayı anlamlandırma" süreçleridir. Hedef; neyin doğru olduğuna dair standartları, değer sıralamalarını, aidiyet hissini, kurumlara duyulan güveni ve geleceğe dair ortak tasavvuru tahrip etmektir.47 Bu yaklaşım, FIMI'yi bir içerik modifikasyonu olmaktan çıkarıp, toplumun ortak yargı alışkanlıklarına yönelik "sistemik bir sabotaj" haline getirmiştir.

3. Avrupa Birliği Dijital Caydırıcılık ve FIMI Araç Kutusu: Avrupa Birliği (AB), 2025 ABD Ulusal

Güvenlik Stratejisi sonrası değişen güvenlik şemsiyesine karşı kendi hibrit savunma kalkanını oluşturmaya hız vermiştir.48 Geleneksel siber saldırılar ile FIMI operasyonları arasındaki yapay ayrım ortadan kalkmıştır. AB Dijital Hizmetler Yasası (DSA) ve yeni yaptırım rejimleri çerçevesinde geliştirilen FIMI Araç Kutusu (FIMI Toolbox), dezenformasyonu yalnızca bir ifade özgürlüğü sorunu olarak değil; dolandırıcılık, yasadışı finansman ve siber suç bağlamında cezai ve idari yaptırımlara tabi bir davranışsal ihlal olarak ele almaya başlamıştır.9 Bu hukuki trend, zararlı anlatıların içeriğinden (content) ziyade, koordine inotantik davranışlara (behavior) odaklanarak liberal demokrasilerin yasal paradokslarını aşmasını sağlamıştır.

4. Kuantum Teknolojileri ile Karşı Tedbirler: Tehditlerin bilişsel seviyeye ulaşması, askeri

sistemlerin fiziksel olarak daha da izole edilmesini gerektirmiştir. NATO Bilim ve Teknoloji Organizasyonu (STO) 2025 yılı raporlarına göre, Kuantum Teknolojileri (QT) bilişsel/siber savaşa karşı en kritik defans hattı olarak görülmektedir.50 Denizcilik Araştırma ve Deney Merkezi (CMRE), uyduların karıştırılabildiği (GPS jamming) ortamlarda kuantum manyetometreler ile eylemsiz hassas navigasyon testleri gerçekleştirmiş; kuantum iletişim ağları ve foton yayılımı aracılığıyla verilerin dış manipülasyondan ve dinlemeden bağımsız olarak güvenli iletimini

sağlamıştır.50 Bu fiziksel güvenlik, komuta kademesinin bilişsel olarak zehirlenmesini engellemenin temel dayanağıdır.

5. Anlamlı İnsan Kontrolü (Meaningful Human Control): Tüm bu otonom saldırı ve savunma

ajanlarının gelişimi, etik ve doktriner bir ikilemi beraberinde getirmiştir.51 Yapay zekâ otonomisinin siber uzayda tetiği çekme yetkisi arttıkça, Birleşmiş Milletler ve NATO gibi platformlarda yapay zekâ destekli FIMI savunmasında "anlamlı insan kontrolünün" nasıl korunacağı ve bağımsız bilimsel değerlendirmelerin nasıl yapılandırılacağı, dönemin en yoğun tartışılan normatif çerçevesi olmuştur.6 Stratejik Sonuçlar ve Gelecek Projeksiyonu Siber-bilişsel kesişimdeki bu çok katmanlı, ampirik ve teorik ekosistem analiz edildiğinde, uluslararası güvenlik mimarisi ve karar alıcılar için hayati stratejik sonuçlar ortaya çıkmaktadır:

1. Ortak Otonom İstihbarat Mimarisinin Kurumsallaşması: FIMI operasyonlarına karşı

parçalı, izole ve manuel istihbarat yapılarıyla mücadele etmek stratejik körlük yaratmaktadır. DISARM çerçevesinin, STIX/TAXII formatları ve Tehdit İstihbarat Platformları üzerinden Müttefik ülkelerin stratejik iletişim birimlerine "makine hızında" entegre edilmesi zaruridir.10 Ortak ve otonom bir taksonomi olmadan, düşmanın OODA döngüsü kırılamaz; zira manuel tespitler geldiğinde, toplum halihazırda bilişsel manipülasyona uğramış olur.

2. Karar Merkezli Doktriner Dönüşüm: bilişsel harp, düşmanın silah sistemlerini değil,

karar vericilerin nörolojik algısını hedefler. Bu sebeple, FIMI ve bilişsel harp operasyonları, geleneksel "bilgi harekatı" statüsünden çıkarılarak, kurumsal eğitim ve savunma vizyonunda "karar merkezli operasyonel konsept" olarak kurumsallaştırılmalıdır.17 Askeri savaş oyunları (wargames) ve simülasyonlar, bilgi alanındaki kirliliğin yarattığı "bilişsel stresörleri" senaryolarına acilen dahil etmelidir.17 Karar koruması ve eylem koruması, askeri eğitimin ayrılmaz bir parçası olmalıdır.5

3. Kurumlararası Ortak Görev Güçlerinin (JIATF) Gerekliliği: FIMI tehdidi hibrit karakteri

gereği; diplomatik meşruiyeti, finansal güvenliği, siber altyapıyı ve toplumsal bütünlüğü aynı anda tahrip eder. Bu asimetrik çok boyutluluğa karşı, yalnızca istihbarat servisleri veya siber askeri komutanlıklarla yanıt verilemez. Devlet departmanlarını (örneğin ABD Dışişleri Bakanlığı), STK'ları, sosyal medya platformlarını, siber güvenlik endüstrisini ve akademi mensuplarını bir araya getiren Kurumlararası Ortak Görev Güçleri (Joint Interagency Task Forces) kurulmalı ve "ağların ağı" (network of networks) felsefesiyle işletilmelidir.2

4. Mavi Takım Sınırlarının Hukuki Olarak Çizilmesi: DISARM Mavi Çerçevesinin sunduğu

önlemler (platformdan hesap kaldırma, algoritmaları düşürme, finansı kesme) otokratik sansür politikaları ile demokratik savunma hatları arasındaki ince çizgide yürümektedir.30 Açık toplumlar, bilişsel saldırıları savuştururken ifade özgürlüğünü

ihlal etmeyen, FIMI araç kutusunda belirtildiği gibi içeriği değil, "davranışı" (yasadışı otomasyon, bot ağları) hedef alan yasal regülasyonları hızla olgunlaştırmak zorundadır.39 Son tahlilde, siber-bilişsel kesişimdeki asimetrik mücadele, toplumların teknolojik altyapılarını korumaktan öte, demokrasiye olan inancı, kolektif hafızayı ve gerçeğin bizatihi kendisini savunma savaşıdır.47 Karşılaşılan tehdit, yapay zekâ aracılığıyla hiper-optimize edilmiş, görünmez ve yıkıcıdır. FIMI aktörlerinin siber altyapıları ile insan bilişi üzerinde yarattığı tahribat, ancak DISARM gibi sistematik, evrensel, çok-ajanlı otonom sistemlerle güçlendirilmiş entegre bir durumsal farkındalık mimarisi ile etkisiz hale getirilebilir.8 Stratejik avantaj, füzeleri ateşleyenlerde değil; toplumların neye inanıp nasıl karar vereceğini saniyeden çok daha kısa sürelerde, görünmez mimariler üzerinden şekillendirebilenlerin ve bunu savuşturabilenlerin elinde olacaktır.

Alıntılanan çalışmalar

1. The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and

Bridging the Gap to Extant Literatures - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/ST O-MP-HFM-361/MP-HFM-361-P13.pdf

2. About us - DISARM Foundation, erişim tarihi Haziran 3, 2026,

https://www.disarm.foundation/about-us

3. Disinformation In Cognitive Warfare, FIMI, Hybrid Threats - The Defence Horizon Journal,

erişim tarihi Haziran 3, 2026, https://tdhj.org/blog/post/disinformation-cognitive-warfare-hybrid/

4. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory

concept - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/

5. Cognitive Warfare: Definition, Framework, and Case Study - arXiv, erişim tarihi Haziran 3,

2026, https://arxiv.org/html/2603.05222v1

6. Health, Human Rights, Humanitarian Action, Heritage-Education-Literacy,

Climate-Environment, Development, Peace - The Sentinel, erişim tarihi Haziran 3, 2026,

https://ge2p2-center.net/wp-content/uploads/2026/03/the-sentinel_-period-endi ng-08-mar-2026.pdf

7. Cognitive Warfare: Generative AI, False Realities, and International Humanitarian Law,

erişim tarihi Haziran 3, 2026, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1156&context=research

8. An Agentic Operationalization of DISARM for FIMI Investigation on Social Media - arXiv,

erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2601.15109v1

9. AMIT blog series - EU CyberNet, erişim tarihi Haziran 3, 2026,

https://www.eucybernet.eu/wp-content/uploads/2025/03/eu-cybernet-expert-se ries-no1-2025-ashkenazi.pdf 10.An Agentic Operationalization of DISARM for FIMI Investigation on Social Media - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2601.15109v3

11. An Agentic Operationalization of DISARM for FIMI Investigation on Social Media - arXiv,

erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2601.15109v2 12.Building Whole-of-Society Resilience Against Foreign Information Manipulation and Interference in Canada - CDA Institute, erişim tarihi Haziran 3, 2026, https://cdainstitute.ca/wp-content/uploads/2026/04/Chobotov-Policy-Paper-202 6.pdf 13."Just Being Born": Assessing and Countering Foreign Information Manipulation and Interference (FIMI) in Japan < Sasakawa USA, erişim tarihi Haziran 3, 2026, https://spfusa.org/publications/just-being-born-assessing-and-countering-foreig n-information-manipulation-and-interference-fimi-in-japan/ 14.HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM - NATO, erişim tarihi

Haziran 3, 2026,

https://www.nato.int/content/dam/nato/webready/documents/deep/Hybrid-threat s-and-hybrid-warfare-ENGLISH.pdf 15.Detecting FIMI: A methodological framework for testing OSINT tools in TTPs detection., erişim tarihi Haziran 3, 2026, https://open-research-europe.ec.europa.eu/articles/6-157

16.Hybrid Threats, Cognitive Warfare, and Psychological Defence - Taiwan Fellowship, erişim tarihi Haziran 3, 2026, https://taiwanfellowship.ncl.edu.tw/files/scholar_publish/2453-ucvlwysesodzuso.p df 17.Cognitive Warfare: Definition, Framework, and Case Study - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2603.05222 18.(PDF) Cognitive Warfare: Definition, Framework, and Case Study - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/401600289_Cognitive_Warfare_Definiti on_Framework_and_Case_Study 19.Research Proposes Metric to Measure Effectiveness of Cyber Cognitive Attacks and Online Disinformation Campaigns - HSToday, erişim tarihi Haziran 3, 2026, https://www.hstoday.us/subject-matter-areas/cybersecurity/research-proposes- metric-to-measure-effectiveness-of-online-disinformation-campaigns/ 20.Quantifying the Engagement Effectiveness of Cyber Cognitive Attacks: A Behavioral Metric for Disinformation Campaigns - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2510.15805 21.Being There: Content, Cognition and Strategic Competition - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/ST O-MP-HFM-361/MP-HFM-361-P14.pdf 22.Definitional ambiguity in cognitive warfare: a critical and systematic conceptual review through ideal-type analysis - Frontiers, erişim tarihi Haziran 3, 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2026.1762571/ pdf 23.Disinformation - DISARM Foundation, erişim tarihi Haziran 3, 2026, https://www.disarm.foundation/disinformation 24.DISARM Foundation, erişim tarihi Haziran 3, 2026, https://www.disarm.foundation/ 25.Disarming disinformation: How EclecticIQ helps you analyze and..., erişim tarihi Haziran 3, 2026, https://blog.eclecticiq.com/disarm-framework 26.Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' - Hybrid CoE, erişim tarihi Haziran

3, 2026, https://www.hybridcoe.fi/wp-content/uploads/2022/11/20221129_Hybrid_CoE_Res earch_Report_7_Disarm_WEB.pdf 27.The Story So Far - DISARM Foundation, erişim tarihi Haziran 3, 2026, https://www.disarm.foundation/brief-history-of-disarm 28.Framework - DISARM Foundation, erişim tarihi Haziran 3, 2026,

https://www.disarm.foundation/framework 29.DISARM Framework - "Mendeleev's table" of information operations and campaigns, erişim tarihi Haziran 3, 2026, https://project-athena.eu/disarm-framework-mendeleevs-table-of-information-operations-and-campaigns/ 30.DISARMFoundation/DISARMframeworks: Master copies of the DISARM frameworks, with generated files to help you explore the data · GitHub, erişim tarihi Haziran 3, 2026, https://github.com/DISARMFoundation/DISARMframeworks/ 31.Mapping the methods of influence: insights from ATHENA's 32 FIMI case studies, erişim tarihi Haziran 3, 2026, https://project-athena.eu/mapping-the-methods-of-influence-insights-from-athenas-32-fimi-case-studies/ 32.Automatic Tagging of Foreign Information Manipulation and Interference Incidents With DISARM Tactics, Techniques, and Procedures - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/6287639/11323511/11343758.pdf 33.Cognitive Warfare Indicators and Warnings Identification Framework - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-377/MP-HFM-377-09.pdf 34.Welcome to DISARM - Disarm Framework Explorer, erişim tarihi Haziran 3, 2026, https://disarmframework.herokuapp.com/ 35.Data analysis using the DISARM Framework | Data Knowledge Hub for Researching Online Discourse, erişim tarihi Haziran 3, 2026, https://data-knowledge-hub.com/docs/data-analysis/04_04_disarm-framework/

36.LLM Agent for Disinformation Detection Based on DISARM Framework - Proceedings of the ICWSM Workshops, erişim tarihi Haziran 3, 2026, https://workshop-proceedings.icwsm.org/pdf/2024_68.pdf 37.Analyzing frameworks to model disinformation attacks in online social networks - idUS, erişim tarihi Haziran 3, 2026, https://idus.us.es/bitstreams/19477544-14a1-4294-a1e2-92f0ea06ef03/download 38.An Agentic Operationalization of DISARM for FIMI Investigation on Social Media, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/399962530_An_Agentic_Operationalization_of_DISARM_for_FIMI_Investigation_on_Social_Media 39.Beyond Disinformation Countermeasures: Building a Response-Impact Framework, erişim tarihi Haziran 3, 2026, https://www.disinfo.eu/publications/beyond-disinformation-countermeasures-building-a-response-impact-framework/ 40.1st EEAS Report on Foreign Manipulation and Interference Threats - OCR of the Document | National Security Archive, erişim tarihi Haziran 3, 2026, https://nsarchive.gwu.edu/media/30068/ocr 41.An Agentic Operationalization of DISARM for FIMI Investigation on Social Media - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2601.15109 42.[□□ □□] An Agentic Operationalization of DISARM for FIMI Investigation on Social Media, erişim tarihi Haziran 3, 2026, https://www.themoonlight.io/ko/review/an-agentic-operationalization-of-disarm-f or-fimi-investigation-on-social-media 43.Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information -war-international-affairs 44.Cognitive Warfare, Disinformation, and Corporate Influence in Europe's Energy Transition: Information Control, Regulation, and Human Rights Implications, erişim tarihi

Haziran 3, 2026,

https://www.acigjournal.com/Cognitive-Warfare-Disinformation-and-Corporate-Influence-in-Europe-s-Energy-nTransition,214045,0,2.html 45.Cognitive Warfare in Historical Perspective: From Cold War Psychological Operations to AI-Driven Information Campaigns - Preprints.org, erişim tarihi Haziran 3, 2026, https://www.preprints.org/manuscript/202512.1596 46.Gamification of Narrative Language and Grassroot Cognitive Warfare - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/commentary/2026/03/gamification-of-narrative-language-and-grassroot-cognitive.html 47.Invisible by design: NATO's 2026 cognitive warfare paper and the crisis of discovery, erişim tarihi Haziran 3, 2026, https://complexdiscovery.com/invisible-by-design-natos-2026-cognitive-warfare -paper-and-the-crisis-of-discovery/ 48.Enter Europe's Cyber Deterrence - CSIS, erişim tarihi

Haziran 3, 2026, https://www.csis.org/analysis/enter-europes-cyber-deterrence 49.4th EEAS Report on Foreign Information Manipulation and Interference Threats - European Union, erişim tarihi Haziran 3, 2026, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf 50.2025 Highlights Report - NATO Science and Technology Organization, erişim tarihi

Haziran 3, 2026,

https://www.sto.nato.int/wp-content/uploads/nato-sto-004-2025-highlights-repo rt-digital-v5-pages.pdf 51.[2504.11486] Designing AI-Enabled Countermeasures to Cognitive Warfare - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2504.11486 52.Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' (prepared in cooperation with Hybrid COE), erişim tarihi Haziran 3, 2026, https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language- and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253

53.How to Lose an Information War in 10 Days - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/how-lose-information-war-10-days Bölüm Değerlendirme ve Derinleştirme Dosyası

Bölüm Değerlendirme ve Derinleştirme Dosyası

Bu bölümün geniş okuması yapılırken FIMI ve DISARM yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası aktör, davranış, içerik, kanal, etki ve karşı tedbir zinciri üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle FIMI ve DISARM alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum

hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece

prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● ● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Siber-Bilişsel Kesişimde FIMI ve DISARM Çerçevesi alanında en güçlü erken uyarı
göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

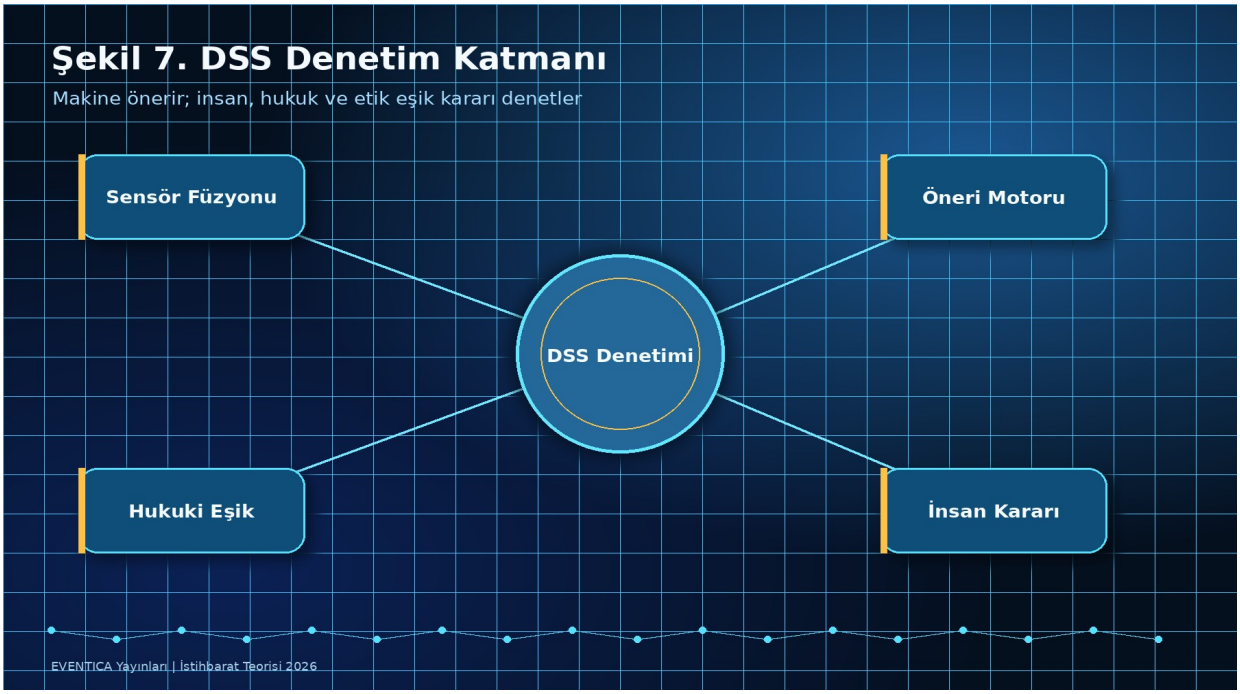
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030'a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 7. Otonom Hedefleme ve Karar Destek Sistemleri



DSS, komutanın kararını desteklediği sürece değerlidir; insan doğrulamasını sembolik hale getirdiği anda fiili otonomi riski doğar.

Şekil 7. DSS içinde insan denetimi, hız ve hukuk filtresi

Tablo 10. DSS tasarımında kontrol matrisi

Kontrol alanı	Gereken mekanizma	Amaç
Veri kökeni	Kaynak ve zaman damgası	Yanlış hedeflemeyi azaltma
Model açıklanabilirliği	Gerekçe ve kanıt izi	Operatör denetimini güçlendirme
Hukuki filtre	IHL/ROE kontrol noktaları	Meşruiyet ve sorumluluk
İnsan onayı	Gerçek, anlamlı ve belgelenmiş onay	Fiili otonomiyi sınırlama

Tablo 10. DSS tasarımında kontrol matrisi Kontrol alanı Gereken mekanizma

Amaç

Veri kökeni Kaynak ve zaman damgası Yanlış hedeflemeyi azaltma Model açıklanabilirliği Gerekçe ve kanıt izi Operatör denetimini güçlendirme Hukuki filtre IHL/ROE kontrol noktaları Meşruiyet ve sorumluluk İnsan onayı Gerçek, anlamlı ve

belgelenmiş onay Fiili otonomiyi sınırlama Otonom Hedefleme ve Karar Destek Sistemleri (DSS): Kinetik Operasyonlarda Hız ve Doğruluk İkilemi

1. Kavramsal Çerçeve Modern savaş alanı, sensörlerin, algoritmaların ve kinetik vurucu

güçlerin eşi görülmemiş bir hızda ve hiper-bağlantılı bir ağ üzerinden entegre olduğu yeni bir paradigmaya geçiş yapmıştır.

Geleneksel askeri doktrinlerin temelini oluşturan savaşın sisli ve sürtünmeli doğası, yapay zekâ (YZ) tabanlı Karar Destek Sistemleri (Decision Support Systems - DSS) ve otonom hedefleme mimarileri ile yeniden tanımlanmaktadır.1 Bu dönüşümün merkezinde, kinetik operasyonların belkemiği olan hedefleme döngüsünün (Targeting Cycle) veya yaygın bilinen

adıyla OODA (Gözlem, Yönelim, Karar, Eylem - Observe, Orient, Decide, Act) döngüsünün zamansal olarak sıkıştırılması stratejisi yatmaktadır.3 OODA döngüsünün yapay zekâ aracılığıyla hızlandırılması, günümüz muharebe alanında bir lüks olmaktan çıkıp kesin bir operasyonel zorunluluğa dönüşmüştür.

Taktiksel avantaj, düşmanın karar alma hızını aşan bir süratte bilgi işleyebilme kapasitesine bağlıdır.3 Ancak bu hızlanma arayışı, askeri stratejide ve uluslararası hukukta köklü bir kriz olan "hız ve doğruluk ikilemi"ni (speed-accuracy trade-off) benzeri görülmemiş bir boyuta taşımaktadır.6 Geleneksel savaşta, bir hedefin tespit edilmesi, doğrulanması, hukuki süzgeçlerden geçirilmesi ve vurulması için gereken zaman, insan bilişinin, analitik süreçlerin ve askeri bürokrasinin doğal kısıtlamaları tarafından belirlenirken; gelişmiş YZ tabanlı sistemler bu süreci saatlerden veya günlerden saniyelere indirmektedir.7 Bu sıkışma, OODA döngüsünün Gözlem (veri toplama) ve Yönelim (veri füzyonu ve analiz) aşamalarını makine hızına çıkarırken, Karar (insan onayı ve yasal denetim) aşamasında devasa bir darboğaz yaratmaktadır.5 Otonom hedefleme sistemleri ile Karar Destek Sistemleri (DSS) arasındaki ontolojik fark, tam da bu darboğazın yönetilmesinde belirginleşir. Tam otonom ölümcül silah sistemleri (Lethal Autonomous Weapons Systems - LAWS), hedefi belirleme ve tetiği çekme kararını doğrudan, hiçbir insan müdahalesi veya onayı olmadan alabilen sistemleri ifade eder.

Buna karşılık, YZ tabanlı Karar Destek Sistemleri (DSS), devasa boyutlardaki çok alanlı (multi-domain) veri setlerini işleyerek insan komutana hedefler veya hareket tarzları (Course of Action - CoA) öneren analitik mimarilerdir.8 Ancak kinetik sahanın acımasız gerçekliğinde, DSS'in makine hızında hedef önerme kapasitesi, insan operatörün bu önerileri bağımsız olarak doğrulama ve hukuki filtrelerden geçirme kapasitesini aştığında, DSS fiili olarak otonom bir karar alıcıya dönüşme riski taşır.7 Hedefleme mimarilerindeki hız ve doğruluk ikilemi; düşmanı gafil avlayacak taktiksel sürat ile Uluslararası İnsancıl Hukuk'a (IHL) uyum sağlayan ve sivil zayiatı önleyen isabetlilik arasındaki son derece hassas, çoğu zaman sıfır toplamlı bir dengeyi temsil etmektedir.11 Bu çerçevede yapay zekâ, Clausewitz'in tanımladığı savaşın "sürtünme" (friction) unsurunu ortadan kaldırmaz; aksine onu insan idrakından çıkarıp algoritmik bir düzleme taşır. Karar vericiler, makinenin sunduğu kusursuz görünen istatistiksel olasılıklara karşı, insan sezgisinin ve yasal sorumluluğun yükünü dengelemek zorundadır.13 Otonom sistemler, savaş alanında yeni veriler üretmekten ziyade, var olan verilerden hareketle tahmine dayalı (predictive) yeni eylem setleri yaratırlar.

Dolayısıyla, hedeflerin belirlenmesinde kullanılan otonom teknolojilerin salt birer araç olmanın ötesine geçerek, bizzat savaşın etiğini ve stratejik sınırlarını belirleyen yapısal aktörlere dönüştüğü bir döneme girilmektedir.

2. Akademik Teoriler YZ tabanlı askeri hedefleme ve karar destek sistemlerinin

entegrasyonu, salt bir mühendislik problemi olmanın ötesindedir. Bu sistemler, bilişsel psikoloji, uluslararası hukuk ve stratejik yönetim teorilerinin kesişiminde yer alan derin ve karmaşık bir teorik altyapı üzerinden analiz edilmelidir.

Otomasyon Sapması ve Algoritma Kaçınması Teorileri (Bilişsel Psikoloji) Makine hızıyla çalışan hedefleme sistemlerinin insan psikolojisi ve karar alma süreçleri üzerindeki en kritik teorik etkisi "Otomasyon Sapması"dır (Automation Bias).7 Otomasyon sapması, komutanların, istihbarat analistlerinin ve silah operatörlerinin, sistemin sunduğu hedefleme önerilerinin ardındaki yapılandırılmamış veriyi ve bağlamı tam olarak anlamadan, algoritmik kararlara aşırı güven duyarak bunları sorgusuz sualsiz kabul etme bilişsel eğilimidir.7 Hızın bir erdem sayıldığı ve hayatta kalmanın saniyelere bağlı olduğu kinetik ortamlarda, karar döngüsünün makine lehine daralması, insanı bağlamsal bir "karar alıcı" olmaktan çıkarıp, sistemin kararlarını hızla onaylayan bir "kauçuk damga"ya (rubber stamp) dönüştürebilir.10 Karar vericinin, sistemin hatalı, orantısız veya yasadışı bir hedefleme önerisinde bulunduğunda bile makinenin daha iyisini bildiğini varsayması, savaş alanında geri döndürülemez trajedilere yol açar.

Bunun tam zıttı spektrumunda yer alan "Algoritma Kaçınması" (Algorithm Aversion) teorisi ise, operatörlerin YZ araçlarına yönelik erken ve yersiz bir güvensizlik geliştirerek, sistemin sunduğu doğru istatistiksel istihbaratı reddetmesi durumudur.16 Savaş alanında tecrübeli komutanların, kendi sezgilerine makinelerden daha fazla güvenmesi, algoritmik avantajın kaybedilmesine neden olabilir. Bu iki bilişsel uç noktanın askeri personel üzerindeki etkisini ölçmek amacıyla, West Point Amerika Birleşik Devletleri Askeri Akademisi'nde 236 askeri öğrenci ve benzer demografiye sahip sivil halk üzerinde yürütülen ampirik bir araştırma, kritik bulgular sunmuştur.

Araştırma, askeri eğitim almış ve yapay zekâ sistemlerinin temellerine aşina olan askeri personelin, sivil halka kıyasla otomasyon sapmasına ve algoritma kaçınmasına daha az eğilimli olduğunu, algoritmik sistemlere karşı daha rasyonel ve iyi kalibre edilmiş bir güven sergilediklerini ortaya koymaktadır.16 Bu durum, YZ'nin savaş alanındaki bilişsel risklerinin, hedefleme sisteminin salt algoritmik tasarımı kadar, operatörün askeri eğitimi, teknolojik

okuryazarlığı ve YZ risk bağlamını anlama düzeyi ile de doğrudan ve nedensel olarak ilişkili olduğunu kanıtlamaktadır.18 Uluslararası İnsancıl Hukuk (IHL) Teorileri: Ayrım ve Orantılılık Hukuki çerçevede, otonom hedefleme sistemleri ve karar destek araçları, Uluslararası İnsancıl Hukuk'un (IHL) iki temel teorik ve pratik direğini ontolojik olarak sarsmaktadır: Ayrım ilkesi (Principle of Distinction) ve Orantılılık ilkesi (Principle of Proportionality).7 Ayrım ilkesi, tarafların meşru askeri hedefler (kombatanlar) ile siviller arasında net, şüpheye yer bırakmayacak bir ayrım yapmasını emreder. YZ modelleri, özellikle makine öğrenmesi ve bilgisayarlı görü algoritmaları, sensörlerden gelen görüntüleri veya iletişim verilerini istatistiksel olarak işleyerek bu ayrımı yapmaya çalışır. Ancak algoritmaların eğitim verilerinde (training data) var olan yapısal önyargılar, demografik dengesizlikler veya "hedef olmayan" sivillere ait verilerin modele dahil edilmemesi, ciddi hedef misidentifikasyonuna (yanlış teşhis) yol açar.7 Hukuki teoride ayrım ilkesi, makinenin piksel eşleştirmesinin ötesinde, kişinin niyetini ve statüsünü (örneğin, elinde silah tutan kişinin bir düşman askeri mi, yoksa evini savunan bir sivil mi olduğunu) bağlamsal olarak yorumlamayı gerektirir. Makinelerin semantik anlama kapasitesinden yoksun oluşu, bu ilkenin salt algoritmik olarak yerine getirilmesini imkansız kılar.

Orantılılık ilkesi (Kural 14) ise, beklenen sivil zayiatın, elde edilecek "somut ve doğrudan askeri avantaja" kıyasla aşırı olmamasını şart koşar.7 Uluslararası Ceza Mahkemesi (ICC) Statüsü ve Cenevre Sözleşmeleri Ek Protokol I (Madde 51 ve 57) uyarınca, orantısız saldırılar savaş suçu teşkil eder. Bir algoritmanın orantılılık hesaplaması yapabilmesi için, "askeri avantaj" gibi soyut, operasyonun geneline yayılan ve yüksek düzeyde hukuki insan yargısı gerektiren bir kavramı matematiksel bir değere indirgemesi gerekir.7 Fransa, İngiltere ve ABD gibi ülkelerin devlet pratikleri, askeri avantajın tekil bir saldırıdan ziyade operasyonun "bütünü" üzerinden (overall military advantage) değerlendirilmesi gerektiğini savunur. Yapay zekâ sistemleri, mikro düzeydeki taktiksel hedefleri saniyeler içinde hesaplayabilirken, makro düzeydeki "bütüncül avantajı" ve sivil yaşamın değerini kodlanmış bir ahlaki çerçeve içinde tartamaz.7 Bu yetersizlik, "Anlamlı İnsan Kontrolü"nün (Meaningful Human Control -

MHC) sadece teorik bir etik gereklilik olmaktan çıkıp, yasal bir hesap verilebilirlik zorunluluğu haline geldiğini göstermektedir.7 Karar Egemenliği ve Enerjetik Paradigma (Decision Sovereignty) 2026 yılı itibarıyla stratejik araştırma kurumlarında (örneğin IEEE ve arXiv üzerinden yayınlanan çalışmalarda) ivme kazanan yeni ve kritik bir teori "Karar Egemenliği"dir (Decision Sovereignty).22 Devletlerin, otonom kabiliyet yarışında geri kalmamak için frontier (sınır ötesi) YZ tedarikçilerinden (örneğin büyük teknoloji şirketlerinden) ticari veya yarı-ticari yapay zekâ

modelleri satın alarak askeri iş akışlarına entegre etmesi, devasa bir stratejik bağımlılık riski doğurmuştur. Akademik literatürde formüle edilen "Tedarikçi Kaynaklı Sınır Kontrolü" (supplier-induced boundary control) tehdit modeli, özel bir şirketin tasarladığı, mülkiyet haklarına sahip olduğu ve kara kutu (black-box) olarak çalışan kapalı kaynak bir modelin, bir devletin askeri eylem onayı, operasyonel eskalasyon politikası ve hedefleme kısıtlamaları üzerinde dolaylı yoldan kontrol sahibi olması riskini tanımlar.22 2026'daki kamuoyuna yansıyan Anthropic-Pentagon anlaşmazlığı ve Project Maven'in tarihsel gelişimi bu teorinin pratik kanıtlarıdır. Bu stratejik açmazı çözmek için "Enerjetik Paradigma" (Energetic Paradigm) olarak adlandırılan teorik bir sistem mimarisi önerilmektedir. Bu yaklaşıma göre, tedarikçiden alınan algoritmik analitik modeller istenildiği zaman değiştirilebilir, tak-çıkar (plug-and-play) bileşenler olarak kalmalıdır.

Ancak komuta yönlendirmesi, operasyonel kısıtlamalar, sistem denetim günlükleri (logging), hedef onayı ve yasal tırmanma (escalation) yetkisi tamamen devlet mülkiyetinde, egemen kurumların kontrolünde olan bir çerçevede (framework) tutulmalıdır.22 Bu sayede, ticari sırların ifşa edilmesine gerek kalmadan karar egemenliği güvence altına alınır.

3. Sistem Mimarisi Otonom hedefleme ve askeri Karar Destek Sistemleri'nin (DSS) fiziksel ve

yazılımsal mimarisi, laboratuvar ortamındaki teorik YZ modellerinden çok farklı dinamiklere sahiptir. Savaş alanının kaotik doğası, fiziksel cihaz limitleri, veri iletişim kısıtlamaları ve yasal zorunluluklar, bu sistemlerin "Çoklu-Paradigma" ve "Uç Bilişim" odaklı tasarlanmasını dikte eder.

Uç Bilişim (Edge Computing) ve Hız-Doğruluk Mühendisliği Modern kinetik operasyonlarda otonom sistemler (örneğin kamikaze dronlar veya ileri gözetleme sensörleri), düşman tarafından yoğun elektronik harp (EW) uygulanan, iletişim ağlarının kesildiği veya karıştırıldığı "elektronik olarak erişime engellenmiş" (denied electronic environments) ortamlarda görev yapmaktadır.6 Bu koşullar altında YZ tabanlı donanımların bulut sunucuları (cloud computing) ile bağlantı kurarak devasa verileri analiz ettirmesi imkansızdır. Bu durum, "Uç Bilişim" (Edge Computing) mimarisini teknik bir zorunluluk haline getirmektedir.6 Uç bilişim, sistemin otonom karar alma, hareket planlama, nesne tanıma ve hedefleme yeteneklerinin doğrudan cihazın üzerindeki donanımlarda (on-board companion computer) hesaplanmasını gerektirir.25 Ancak uç bilişim mimarisi acımasız donanımsal ve enerjetik sınırlamalara tabidir. Gelişmiş derin öğrenme (deep learning) algoritmaları, hedefleri hassas bir şekilde tanımlayabilmek için son derece yüksek işlemci kapasitesi (GPU/TPU) ve

bellek gerektirir, bu da cihazın pil ömrünü sömürür ve görev süresini dramatik şekilde kısaltır.6 Geliştiriciler, hız, menzil ve doğruluk arasında donanım seviyesinde ağır tavizler vermek zorundadır. Sistemi hafifletmek ve enerji tüketimini optimize etmek için aşağıdaki mimari mühendislik teknikleri kullanılır:

1. Model Sıkıştırma (Compression): YZ modelinin gerektirdiği ağırlıkları depolamak veya

iletmek için gereken bit sayısını düşürerek modelin hızını ve enerji verimliliğini artırır, ancak bu süreçte piksel hassasiyeti ve doğruluk oranından belirli oranlarda feragat edilir.6

2. Budama (Pruning): YZ sinir ağındaki hedef belirlemede istatistiksel olarak daha az ağırlığa

sahip, nispeten önemsiz algoritmik düğümlerin (nodes) kalıcı olarak sistemden çıkarılması işlemidir. Sistem hızlanır, daha az kaynak tüketir ancak "öngörülemeyen uç vakalarda" (edge cases) sivil-asker ayrımını yapma kabiliyeti tehlikeye girer.6

3. Paralel Hesaplama (Parallel Computing): Donanım sınırlarını aşmak için tek ve ağır bir

işlemci kullanmak yerine, karmaşık görüntü işleme ve hedefleme görevlerinin düşük güç tüketen birden fazla mikro işlemciye dağıtılarak eşzamanlı çalıştırılmasıdır.6 Çoklu-Paradigma Hedefleme ve Karar Destek Mimarisi Modern askeri Karar Destek Sistemleri'nin (DSS) yazılım mimarisi, hukuki güvenilirlik ve tutarlılık sağlamak amacıyla, sadece kapalı kutu olarak çalışan uçtan uca makine öğrenmesi (end-to-end learning) modellerine dayanmaz. Gelişmiş mimariler, kural tabanlı çıkarım sistemlerini (rule-based reasoning) ve analitik yapay zekâyı birleştiren "Çoklu-Paradigma" yaklaşımları kullanır.8 Bu yapı, Karar Egemenliği teorisi ile uyumlu çalışarak, İstihbarat Hazırlığı (IPB) aşamasından görev icrası ve sonrasına kadar operasyonel yaşam döngüsünün (operational lifecycle) tüm safhalarını kapsar.8

Mimari Katman / İşlevsel Kullanılan Temel Savaş Alanı Paradigma Sorumluluk Teknolojiler

Entegrasyonu ve Avantajı Durumsal Çoklu kaynaklardan GNSS, IMU İnsan algısını aşan Farkındalık / Veri gelen (Uydu, İHA, (Ataletsel Ölçüm), veri kirliliğinin Füzyonu Katmanı Sinyal İstihbaratı) LiDAR (3D temizlenmesi, devasa boyutlardaki Haritalama), Radar, OODA döngüsünün karmaşık verilerin Monoküler Gözlem (Observe) eşzamanlı Kameralar, fazının saniyelere birleştirilmesi ve Semantik İletişim indirilmesi. süzülmesi. Ağları 27 Uçtan Uca Desen tanıma Derin Öğrenme Düşük topografik Öğrenme (Pattern Sinir Ağları, karmaşada veya (End-to-End ML) recognition), Hedef Görüntü İşleme, hedef Katmanı

önceliklendirme, Bilgisayarlı Görü yoğunluğunda Hareket planlama (Computer Vision) hedeflerin yüksek (Motion planning), algoritmaları 20 hızda Dinamik rota sınıflandırılması ve oluşturma. analiste sunulması.

Kural Tabanlı Alt makine Deterministik Sisteme hukuki Mantık öğrenmesi mantık kapıları, izlenebilirlik (Rule-based katmanından gelen Önceden katılması, reasoning) önerilerin programlanmış katı otomasyon Katmanı Uluslararası hukuki ve coğrafi sapmasına İnsancıl Hukuk kısıtlamalar (automation bias) (IHL) kurallarına ve (hard-wired limits) 7 karşı filtre Angajman oluşturulması, sivil Kurallarına (RoE) hedeflerin uygunluk taraması. reddedilmesi.

Komuta ve Sistem hiyerarşisi, 5G/6G İletişim Taktik seviyedeki uç Otonom insan onayı Protokolleri, Karar verilerin Orkestrasyon (human-in-the-loop) Matrisleri, Metadata operasyonel komuta Katmanı denetimi, çoklu Günlükleme merkezlerine (örn. drone sürülerinin Modülleri 7 Delta sistemine) (TADVN) aktarılması ve nihai haberleşmesi ve eylem onayının senkronizasyonu. alınması.

4. Gerçek Dünya Vakaları Uygulamalı stratejik analiz bağlamında, 2020 sonrası çatışmalarda

yapay zekâ tabanlı hedefleme ve Karar Destek Sistemleri'nin (DSS) pratik evrimi üç ana coğrafi ve stratejik tiyatro üzerinden incelenmelidir: İsrail'in Orta Doğu operasyonları, Ukrayna'daki konvansiyonel savaş ve ABD/NATO ittifakının küresel güç projeksiyonu.

İsrail: Hedef Üretim Fabrikası Olarak YZ (Gospel, Lavender ve Where's Daddy?) İsrail ordusunun (IDF) özellikle 2021 (Unity Intifada) ve 7 Ekim 2023 sonrasında Gazze Şeridi'nde yürüttüğü operasyonlar, yapay zekânın kitlesel bir "hedef üretme fabrikası" olarak kullanıldığı ve hız-doğruluk ikileminin en yıkıcı sonuçlarının gözlemlendiği bir

laboratuvara dönüşmüştür.2 İsrail Askeri İstihbarat Birimi 8200 tarafından geliştirilen bu sistemler, hedefleme süreçlerini tamamen değiştirmiştir.

● ● The Gospel (Habsora): Bu sistem doğrudan insanları hedef almaz; makine öğrenmesi

kullanarak binalar, altyapılar ve yapılar (nesneler) üzerine odaklanır.9 Gospel; uydu görüntüleri, siber istihbarat, telefon dinlemeleri ve insani istihbaratı devasa bir veri havuzunda çapraz referanslar ile birleştirir. Önceden onaylanmış hedeflerin kalıplarını bulup, bu kalıpları yeni yapılarla eşleştirir. Önceleri yılda 50 nitelikli hedef çıkarabilen insan analistlerin aksine, Gospel günde 100 potansiyel bombardıman hedefi önerebilecek kapasiteye ulaşarak hedefleme döngüsünü inanılmaz bir hıza taşımıştır.20

● Lavender: Gospel'in aksine, Lavender doğrudan insanları "hedef" olarak derecelendiren otonom destekli bir akıllı veritabanıdır.9 Bireylerin

alışkanlıklarını, lokasyonlarını ve sosyal bağlantılarını analiz ederek Hamas veya Filistin İslami Cihad örgütü ile olan bağlarını istatistiksel olarak puanlar. Sistemin, çatışmanın ilk haftalarında sivil-asker analizini otomatize ederek 37.000'den fazla bireyi hava saldırıları için hedef olarak önerdiği rapor edilmiştir.2

● Where's Daddy? (Babam Nerede?): İnsan istihbaratı ile belirlenen veya Lavender tarafından önerilen şüphelilerin lokasyonlarını izleyen konum tabanlı bir uygulamadır.

Sistem, hedef birey aile evine veya belirli bir coğrafi koordinata girdiğinde hava kuvvetlerine otomatik uyarı göndererek, güdümsüz bombalar ile saldırı planlanmasını kolaylaştırır.17

● Sistemsel ve Etik Arızalar: Bu üçlü mimarinin kullanımı, savaş alanında otomasyon sapmasının (automation bias) ders kitabı niteliğinde bir örneğidir. Komutanların makine onaylarına o kadar bağımlı hale geldiği iddia edilmektedir ki, insan operatörlerin bir Lavender hedefini onaylamak için ortalama sadece "birkaç saniye" harcadığı, yani fiilen bir "kauçuk damga" (rubber stamp) görevi gördüğü belirtilmiştir.20 Dahası, makine öğrenmesi modelinin eğitildiği veritabanında sadece onaylanmış terör hedeflerinin profilleri bulunduğu, "hedef olmayan" sivil verilerin sisteme öğretilmek üzere saklanmadığı (discard edildiği), bunun da sistemde yapısal bir önyargıya (bias) yol açarak sivilleri yüksek oranda hedef olarak etiketlemesine neden olduğu açığa çıkmıştır.20 IHL kurallarının açık ihlali, teknolojinin hatasından ziyade, angajman kurallarının hız uğruna esnetilmesinden kaynaklanmıştır.31 Ukrayna: Dağıtık Ağlar, Delta Sistemi ve Otonom Terminal Güdüm Ukrayna cephesi, YZ hedefleme sistemlerinin, asimetrik bir güç unsuru olarak yoğun elektronik harp (EW) şartlarında ve dağıtık (decentralized) birimler arasında nasıl yaratıcı bir şekilde adapte edildiğinin göstergesidir.32

● Delta Savaş Yönetim Sistemi ve Griselda: Ukrayna, sahadaki tüm operasyonları koordine etmek için "Delta" adında dijital bir savaş yönetim sistemi kullanmaktadır. Delta'yı besleyen temel unsur, "Griselda" adlı YZ yazılımıdır. Griselda;

açık kaynaklar, uydular ve dronlardan gelen kaotik veriyi 30 saniye gibi kısa bir sürede işleyerek gerçek zamanlı ve doğrulanmış istihbarat olarak Delta'ya yükler.32 Amerikan yazılım devi Palantir'in algoritmaları da bu veri füzyonuna entegre edilerek, komutanlara benzersiz bir durumsal farkındalık operasyon haritası sunar.32

● GIS Arta ve Kropyva: Sivil programcılar tarafından geliştirilen bu uygulamalar, savaşın başından beri "Topçuların Uber'i" olarak işlev görmektedir. Hedef koordinatları sisteme girildiğinde, sistem en uygun konumdaki topçu bataryasını seçer ve saniyeler içinde atış verilerini hesaplayarak iletişime geçer, manuel atış hesaplama sürelerini minimize eder.32

● Saker Scout ve Otonom Sistemler (FPV): Rusya'nın Ukrayna dronlarını düşürmek için uyguladığı yoğun GPS engelleme ve radyo sinyali karıştırma

(jamming) taktiklerine karşı, Ukrayna uç bilişim (edge computing) destekli "Saker Scout" drone'larını kullanmaktadır.32 Bağlantı kopsa dahi cihazın üzerindeki yapay zekâ, otonom olarak terminal güdüm (terminal guidance) moduna geçer. Optik kameraları ile çevreyi tarar ve 64 farklı Rus askeri hedef/araç türünü veri tabanından eşleştirerek (bağımsız hedef tespiti) angaje olabilir.32 Rusya'nın "Lancet-3M" ve ABD menşeli "Switchblade 300" mühimmatları da elektronik harpten korunmak için benzer uç terminal güdüm otonomisi sergilemektedir.34 Ukrayna ayrıca, yapay zekâ destekli otonom drone sürüleri (swarm) geliştiren "Swarmer" girişimi ile koordineli çoklu saldırı yetenekleri üzerinde çalışmaktadır.32 ABD, NATO ve AUKUS:

Project Maven, Replicator ve Makro-Stratejik Rekabet

- ● Project Maven: ABD Savunma Bakanlığı'nın (DoD) YZ entegrasyonu konusundaki amiral

gemisi olan Project Maven (2017), sensörlerden ve uydulardan gelen devasa video/görüntü verilerini analiz eden bilgisayarlı görü algoritmalarıdır. 2024 yılı itibarıyla Project Maven algoritmaları, Yemen'deki roket fırlatıcılarının tespitinde, Suriye ve Irak'taki hedeflerin daraltılmasında ve Kızıldeniz'deki Husilere ait yüzey gemilerinin otonom tespitinde aktif olarak kullanılmıştır.29 Project Maven'in başarısı coğrafyaya oldukça bağımlıdır; çöller ve makiler gibi topografik karmaşıklığın az olduğu bölgelerde mükemmele yakın nesne teşhisi yaparken, kentsel alanlarda etkinliği azalmaktadır.29

● Replicator İnisiyatifi: ABD'nin, Çin'in Asya-Pasifik'teki (Indo-Pacom) kitlesel ve sayısal askeri avantajını dengelemek amacıyla başlattığı stratejik bir hamledir. Replicator, hava, kara, deniz ve denizaltı alanlarında on binlerce düşük maliyetli, YZ destekli, otonom ve harcanabilir (attritable) dron sürüsünü kısa süre içinde konuşlandırmayı hedefler.6 Bu projenin başarısı, sistemlerin insan onayı olmaksızın koordine olabilmesi için uç bilişim (edge computing) kabiliyetlerinin sınırlarına ulaşmasına bağlıdır.24

● AUKUS Pillar 2 ve NATO Entegrasyonu: AUKUS anlaşması kapsamında ABD, Birleşik Krallık ve Avustralya, P-8A deniz karakol uçakları üzerinden otonom denizaltı savar YZ algoritmaları ve sonobuoy veri analizi sistemleri geliştirmektedir.41 Benzer şekilde NATO, YZ destekli Karar Destek Sistemleri'ni ittifakın bel kemiği yapmak istese de, üye devletler arasında veri paylaşım kalitesi ve sistem birlikte çalışabilirliği (interoperability) konusunda büyük aşmazlar yaşamaktadır.42

5. Mekanizma Analizi: Hız ve Doğruluk İkileminin Yapısal Doğası Hedefleme süreçlerindeki

otonom mekanizmalar analiz edildiğinde, savaşın Clausewitzci doğasındaki zorlukların ("savaşın sisi" ve "sürtünme") yapay zekâ ile sihirli bir şekilde ortadan kalkmadığı, aksine dijitalleşip hızlanarak form değiştirdiği açıkça görülmektedir.13 Karar Destek

Sistemleri'nin (DSS) mekanik iç işleyişi, temel askeri mantıkta yeni fay hatları yaratmaktadır. OODA döngüsünün işleyiş mekanizması, geleneksel olarak komuta kademesinin düşmandan önce karar alabilmesini hedefler. YZ, yapılandırılmamış devasa sahadan gelen veriyi (radyo sinyalleri, drone termal izleri) istatistiksel kümelere ayırarak hızla "olası hedeflere" dönüştürür.

Ancak pratik mekanizmada bu durum, bir çözüm olmaktan ziyade yeni bir darboğaz (bottleneck) yaratır. İstihbarat döngüsündeki sınırlayıcı unsur, tarih boyunca süregelen "hedef bulamama" sorunundan çıkıp, makinenin saniyeler içinde ürettiği binlerce potansiyel hedefi "doğrulayacak insan zamanının olmaması" sorununa evrilmiştir.9 Komutanların önüne yığılan bu ardı arkası kesilmeyen sentetik hedefler, savaşın zaten stresli olan ortamında bilişsel bir aşırı yükleme (cognitive debt) yaratır ve otomasyon sapmasının (automation bias) mekanik temelini oluşturur.7 Buna ek olarak, yapay

zekânın çevreyi algılama mekanizması fiziksel kısıtlamalara ve dışsal manipülasyonlara son derece açıktır:

1. Topografik ve Çevresel Sınırlılıklar: Bilgisayarlı görü (Computer Vision) algoritmaları;

kentsel çatışma alanları (urban warfare) gibi üç boyutlu yapıların, termal, görsel ve işitsel "dağınıklığın" (clutter) yüksek olduğu, sivil ve askeri unsurların iç içe geçtiği bölgelerde doğruluk oranını ciddi şekilde kaybeder.29 Çölde başarılı olan bir algoritma (örneğin Project Maven), Halep veya Gazze gibi bir şehir dokusunda sivil araçları askeri konvoylarla karıştırabilir.

2. Siber Zaafiyetler ve Veri Zehirlenmesi (Data Poisoning): Otonom hedefleme mimarileri,

doğası gereği geniş siber saldırı yüzeylerine (attack surface) sahiptir.44 Yalnızca geleneksel hackleme değil, sistemin eğitim verilerine sızarak algoritmik modeli içeriden bozmayı hedefleyen "veri zehirlenmesi" ve fiziksel nesnelerin üzerine yapıştırılan özel etiketlerle YZ kamerasını kör eden manipülasyon saldırıları (adversarial AI), mekanizmanın en büyük zaafiyetleridir.3 Düşman birimler bu sayede yanlış hedeflerin (örneğin hastanelerin) sistem tarafından meşru bir askeri tesis gibi algılanmasını sağlayabilir.

3. Makine Öğrenmesi Güven Aralıkları (Confidence Intervals) ve Kara Kutu

Problemi:

Gelişmiş derin öğrenme sistemleri kesinliklere göre değil, istatistiksel olasılıklara göre çalışır. Sistem bir hedefin "düşman unsuru" olma ihtimalini örneğin %85 olarak belirlediğinde, geriye kalan %15'lik yanılma payı, Uluslararası İnsancıl Hukuk'un (IHL) gerektirdiği "haklı beklenti" (bona fide expectation) standardını ne kadar karşılayacaktır? 7 YZ, bu karar

mekanizmasını insan tarafından anlaşılamaz bir "kara kutu" (black-box) içinde yürüttüğü için komutanların mantıksal bir değerlendirme yapması imkansız hale gelir.7 Özellikle uç bilişimde donanım kaynaklarını korumak için sıkıştırma (compression) ve budama (pruning) teknikleri kullanıldığında, bu yanılma payı daha da artarak mekanizmanın operasyonel riskini katlar.6

6. Trend Analizi (2020–2026) 2020 yılından günümüze dek, askeri yapay zekâ ve Karar

Destek Sistemleri, niş deneysel projeler statüsünden çıkıp, küresel stratejik savaş mimarilerinin bel kemiğine doğru baş döndürücü bir hızla evrilmiştir.

Dönem / Yıl Eşik Olay ve Baskın Stratejik Savaş Alanı Teknolojik Trend Göstergesi ve

İnovasyon Etkisi

2020 - 2021 Libya (Kargu-2 YZ'nin izleme Sensörden Dronu), İsrail'in (surveillance) odaklı vurucuya giden "Unity Intifada" pasif kullanımından, sürecin operasyonları (İlk aktif kinetik (sensor-to-shooter) YZ Savaşı) hedefleme alanına ilk defa dijital olarak adım atması.

daraltılması ve veri Otonom angajman füzyonunun tartışmaları. denenmesi.2 2022 - 2023 Ukrayna-Rusya Merkezi olmayan Taktik seviyede Savaşı: GIS Arta, (decentralized) YZ durumsal farkındalık Delta, Kropyva ağlarının, için sivil-asker YZ sistemlerinin geleneksel Sovyet füzyonu ve şiddetli sahaya inmesi ağır siklet askeri elektronik harbe doktrinlerine karşı (jamming) karşı asimetrik güç otonom uç (edge) çarpanı olarak hedefleme kullanılması. çözümlerine (Saker Scout vb.) geçiş.32 2023 - 2024 Gazze: İsrail'in YZ sistemlerinin Operatörler Gospel, Lavender hedef keşfinden üzerinde YZ ve Where's Daddy çok, kitlesel imha otomasyon sistemlerini tam operasyonlarını sapmasının ölçekli kullanması besleyen (automation bias) endüstriyel bir yıkıcı

etkilerinin "hedef üretim uluslararası fabrikası"na kamuoyuna dönüştürülmesi. yansıması; yüksek oranda sivil can kayıpları ve IHL prensiplerinin ihlali.2 2024 - 2026 ABD Project Teknolojik büyük Devletlerin büyük Maven'in Ortadoğu güç rekabeti (US vs. askeri altyapılardan yayılımı, AUKUS Çin). Harcanabilir ziyade, yazılım Pillar 2 denizaltı (attritable) otonom tabanlı mühimmat programı, ABD silah sürülerinin sürülerine yatırım Savunma Bakanlığı (swarm) caydırıcılık yapması. Savaş Replicator İnisiyatifi unsuru olarak alanının operasyonel makro-otomasyona doktrine geçişi.6 entegrasyonu.

2026 ufku, Üretken Yapay Zekâ (Generative AI) ve Büyük Dil Modelleri'nin (LLM), karar destek mimarilerine entegre edildiği tamamen yeni bir döneme işaret etmektedir.28 Bu entegrasyonun amacı, insan operatörlerin son derece karmaşık semantik veriler üzerinden

savaş alanı hakkında doğal dilde hızlı sorgulamalar yapabilmesini sağlamaktır. Ancak bu durum, üretken modellerin bilinen yapısal sorunu olan "sistem halüsinasyonları" ve prompt enjeksiyonları (prompt injection) gibi yepyeni siber açıklara neden olarak, otonom kararların doğruluğunu radikal bir şekilde tehdit edecektir.27

7. Stratejik Sonuçlar Yapay Zekâ (YZ) destekli Karar Destek Sistemleri (DSS) ve otonom

hedefleme mimarilerindeki hiper-hızlı teknolojik ilerleme, önümüzdeki on yıllar boyunca askeri doktrin, uluslararası hukuk, caydırıcılık politikaları ve ittifak yönetimi açısından sistemik stratejik sonuçlar doğurmaktadır.

Birinci Stratejik Sonuç: Kriz Eskalasyonu ve Savaş Eşiğinin Düşmesi OODA döngüsünün makine hızında daraltılması ve algoritmik mantığın savaşın taktiksel yönetimini devralması, uluslararası kriz anlarında saniyeler içinde kontrolden çıkan "çarpışma" (flash crash) senaryolarına zemin hazırlamaktadır. Otonom savunma ve erken uyarı sistemlerinin, düşman algılayıcılarından gelen belirsiz öncül işaretleri anında kesin bir tehdit olarak yorumlaması ve insan idrakının henüz olan biteni kavrayamadığı hızda önleyici kinetik saldırılar önermesi (veya başlatması), düşük yoğunluklu çatışmaları saatler içinde makro-bölgesel savaşlara dönüştürebilir.7 Makinelerin insan zihnine özgü "doğal riskten kaçınma" veya "korku" duygularına sahip olmaması, savaş başlatma eşiğini (threshold for war) tehlikeli ölçüde düşürür.

NATO'nun güncel stratejik değerlendirmeleri, otonom sistemlerin hedef misidentifikasyonu yapmasının ve veri kirliliğine maruz kalmasının, nükleer tırmanma (nuclear escalation) eşiklerini de istikrarsızlaştırabileceği uyarısında bulunmaktadır.44 İkinci Stratejik Sonuç: Hesap Verilebilirlik Boşluğu ve Anlamlı İnsan Kontrolü (MHC) Bir yapay zekâ algoritmasının veya kod bloğunun hukuki şahsiyeti yoktur; dolayısıyla savaş suçlarında aranan en temel ilke olan "kasıt" (mens rea) oluşturamaz, bir mahkeme karşısına çıkarılamaz veya hapse atılamaz.7 YZ tabanlı Karar Destek Sistemlerinin ürettiği yüz binlerce hedefin vurulması sonucunda meydana gelen büyük ölçekli bir katliamda suç; o algoritmayı tasarlayan sivil mühendislere mi, hedef onayı veren "otomasyon sapması" mağduru taktik komutana mı, yoksa sistemi ihraç eden ticari firmaya mı aittir? Bu "Hesap Verilebilirlik Boşluğu" (Accountability Gap), modern orduların uluslararası meşruiyetini kökten sarsan en büyük stratejik krizdir. Çözüm, uluslararası kamuoyunda tartışılan "Anlamlı İnsan Kontrolü" (Meaningful Human Control - MHC) prensibinin soyut bir etik kavram olmaktan çıkarılarak,

askeri mimarilere donanımsal ve yazılımsal olarak gömülmesidir.7 Bunun sağlanması için şu somut denetim mekanizmaları operasyonel zorunluluk olmalıdır:

- ● Hedefleme sürecinin başlangıcından sonuna kadar her aşamasında, insanın bağımsız

karar verebileceği nihai bir reddetme (veto) yetkisinin ve sistem sınırlarının (hard-wired limits) korunması.7

● Operasyonel karar günlüklerinin (metadata log) kriptografik olarak kayıt altına alınarak, makinenin sunduğu seçenekler arasından komutanın hangisini, hangi veriye dayanarak seçtiğinin yıllar sonra bile takip edilebileceği "Uçtan Uca Sorumluluk Matrisleri"nin (End-to-End Responsibility Matrix) zorunlu kılınması.7
● Her YZ sisteminin devreye alınmadan önce ve periyodik olarak, hedef sapmalarına karşı bağlayıcı yasal incelemelere (recurring legal reviews) tabi tutulması.7 Üçüncü Stratejik Sonuç: NATO İttifak İçi Uyum (Interoperability) ve Teknolojik Bağımlılık ABD'nin (Project Maven, Replicator) ve AUKUS müttefiklerinin (Birleşik Krallık, Avustralya) yapay zekâ alanında kendi ekosistemlerini hızla kurması, NATO içindeki dengeleri sarsmaktadır.39 İttifakın gelecekteki en büyük sınaması, üye devletler arasında otonom teknolojilerde asgari standartların belirlenmesi, veri kalitesi, model eğitimi ve ağ güvenliği açısından birlikte çalışabilirliğin (interoperability) sağlanmasıdır.42 Teknolojik kapasitesi yüksek üyeler yapay zekâ verileriyle hareket ederken, ittifakın geri kalanının bu ağları okuyamaması (legacy sistem uyumsuzlukları), kriz anlarında koalisyon güçleri arasında koordinasyonsuzluğa ve trajik "dost ateşi" (friendly fire) vakalarına zemin hazırlayabilir.14 Ayrıca, gelişmiş teknolojilere sahip olmayan devletlerin, müttefik şirketlerden "sınırlandırılmış kapalı algoritmalar" satın alması, karar alma süreçlerinde ticari şirketlere bağımlı (decision sovereignty kaybı) olmalarına yol açacaktır.23 Özetle, Otonom Hedefleme ve Karar Destek Sistemleri; karar alma mekanizmalarını bilişsel olarak insanüstü bir sürate ulaştırarak, taktiksel savaşın tüm matematiksel parametrelerini baştan tanımlamaktadır.

Ancak "hız ve doğruluk" arasındaki amansız sıfır-toplamlı yarışta, orantısız bir şekilde hızı tercih etmek, askeri aygıtın topografik veya elektronik karmaşalar karşısında sadece "çok daha hızlı hata yapmasına" neden olmaktadır. Bu sistemik ikilemin çözümü, donanımsal limitleri zorlayan daha vahşi algoritmalar tasarlamaktan geçmez. Gerçek çözüm, devletlerin egemen komuta haklarını koruyabileceği "Karar Egemenliği" mimarilerinin uygulandığı, insan muhakemesini makinenin cazibesinden arındıracak kullanıcı arayüzlerinin geliştirildiği ve Uluslararası İnsancıl Hukuk'un (IHL) sadece bir uyarı metni olarak değil, algoritmanın donanımsal bir filtresi olarak entegre edildiği melez (çoklu-paradigma) yapılara geçilmesini zorunlu kılmaktadır. Savaşın geri dönülemez bir şekilde makineleştiği bu yeni çağda stratejik

zafer, veriyi en hızlı işleyen tarafın değil; bu amansız hızı rasyonel, yasal ve bağlamsal bir şekilde insan kontrolünde tutabilen tarafın olacaktır.

Alıntılanan çalışmalar

1. Technological Evolution on the Battlefield - CSIS, erişim tarihi Haziran 3, 2026,
https://www.csis.org/analysis/chapter-9-technological-evolution-battlefield

2. The proliferation of AI-enabled military technology in the Middle East, erişim tarihi
Haziran 3, 2026,

https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferation- of-ai-enabled-military-technology-in-the-middle-east/

3. Understanding Adversarial AI: The Military Lens | Future Forge - Defence, erişim tarihi
Haziran 3, 2026,

https://theforge.defence.gov.au/article/understanding-adversarial-ai-military-lens

4. GC REAIM Expert Policy Note Series: Mitigating the Risks of AI-Driven OODA Loops in
Military Decision-Making, erişim tarihi Haziran 3, 2026,
https://hcss.nl/wp-content/uploads/2025/04/Raska.pdf

5. Gaining a Cognitive Advantage: Artificial Intelligence (AI) as a Decision Support System

(DSS) - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/pdfs/AD1177825.pdf

6. The Autonomous Arsenal in Defense of Taiwan: Technology, Law, and Policy of the

Replicator Initiative | The Belfer Center for Science and International Affairs, erişim tarihi Haziran 3, 2026, https://www.belfercenter.org/replicator-autonomous-weapons-taiwan

7. Military AI Challenges Human Accountability - CIP, erişim tarihi Haziran 3, 2026,

https://internationalpolicy.org/publications/military-ai-challenges-human-accountability/

8. Architecture of an AI-Based Automated Course of Action Generation System for Military

Operations - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.20862v1

9. Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the..., erişim tarihi Haziran

3, 2026, https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/ 10.The Effect of Military AI on Contemporary Battlefields | Carnegie..., erişim tarihi Haziran 3, 2026, https://carnegieendowment.org/research/2026/05/the-effect-of-military-ai-on-contemporary-battlefields

11. The Use of the 'Lavender' in Gaza and the Law of Targeting: ai-Decision Support Systems

and Facial Recognition Technology in - Brill, erişim tarihi Haziran 3, 2026, https://brill.com/view/journals/ihls/16/2/article-p336_003.xml 12.Artificial intelligence in military decision-making: supporting humans, not replacing them, erişim tarihi Haziran 3, 2026, https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-dec ision-making-supporting-humans-not-replacing-them/

13.Artificial Intelligence-Enabled Military Decision-Making Process - Marine Corps

University, erişim tarihi Haziran 3, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JA MS-vol-16-no-2/Artificial-Intelligence-Enabled-Military-Decision-Making-Process/ 14.The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare - Geneva Centre for Security Policy (GCSP), erişim tarihi Haziran 3, 2026, https://www.gcsp.ch/sites/default/files/2024-12/geneva-paper-34-24.pdf 15.Code, Command, and Conflict: Charting the Future of Military AI - Belfer Center, erişim tarihi Haziran 3, 2026, https://www.belfercenter.org/research-analysis/code-command-and-conflict-chartin g-future-military-ai 16.[2604.04333] What is Human in Judgment? Comparing Automation Bias and Algorithm Aversion Between the United States Military Academy and the General Public - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2604.04333 17.Incident 672: 'Lavender' and 'The Gospel' AI Systems Reportedly Used in Gaza Targeting Operations with Civilian Harm Allegations, erişim tarihi Haziran 3, 2026, https://incidentdatabase.ai/cite/672/ 18.What is Human in Judgment? Comparing Automation Bias and Algorithm Aversion Between the United States Military Academy and the General Public - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.04333v2 19.The Use of the 'Lavender' in Gaza and the Law of Targeting: ai-Decision Support Systems and Facial Recognition Technology in - Brill, erişim tarihi Haziran 3, 2026, https://brill.com/view/journals/ihls/16/2/article-p336_003.xml?language=en

20.AI-assisted targeting in the Gaza Strip - Wikipedia, erişim tarihi Haziran 3, 2026, https://en.wikipedia.org/wiki/AI-assisted_targeting_in_the_Gaza_Strip 21.Bias in Military

Artificial Intelligence - SIPRI, erişim tarihi Haziran 3, 2026, https://www.sipri.org/sites/default/files/2024-12/background_paper_bias_in_military_ai_0.pdf 22.Preserving Decision Sovereignty in Military AI: A Trade-Secret-Safe Architectural Framework for Model Replaceability, Human Authority, and State Control - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.20867v1 23. [2604.20867] Preserving Decision Sovereignty in Military AI: A Trade-Secret-Safe Architectural Framework for Model Replaceability, Human Authority, and State Control - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2604.20867 24.Revolutionizing Military Drones: The Shift to Edge Computing, erişim tarihi Haziran 3, 2026, https://blog.roninsgrips.com/revolutionizing-military-drones-the-shift-to-edge-computing/ 25.Towards Robust Autonomous Landing Systems: Iterative Solutions and Key Lessons Learned - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.12176v2 26.Towards Robust Autonomous Landing Systems: Iterative Solutions and Key Lessons Learned - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2505.12176v1 27.A Communication-Centric 6G–LLM Architecture for Scalable Tactical Autonomous Defense Vehicle Networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2606.01312v1 28.A Communication-Centric 6G-LLM Architecture for Scalable Tactical Autonomous Defense Vehicle Networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2606.01312 29.The Middle East's AI Warfare Laboratory, erişim tarihi Haziran 3, 2026, https://warontherocks.com/the-middle-easts-ai-warfare-laboratory/ 30.Understanding how Israel uses 'Gospel' AI system in Gaza bombings - FRANCE 24 English, erişim tarihi Haziran 3, 2026, https://www.youtube.com/watch?v=E8e2g7CfXAA 31.US Military Leans Into AI for Attack on Iran, But the Tech Doesn't Lessen the Need for Human Judgment In War, erişim tarihi Haziran 3, 2026,

https://www.gatech.edu/news/2026/03/11/us-military-leans-ai-attack-iran-tech-doe snt-lessen-need-human-judgment-war 32.A Lesson in AI from Ukraine - Human Security Centre, erişim tarihi Haziran 3, 2026, https://www.hscentre.org/uncategorized/lesson-ai-ukraine/ 33.Emerging and Disruptive Technologies Transform, but Do Not Lift, the Fog of War – Evidence from Russia's War on Ukraine - Belfer Center, erişim tarihi Haziran 3, 2026, https://www.belfercenter.org/sites/default/files/2025-10/2024-09-29kunertova-herz ogfnduets.pdf 34.analytical digest ukrainian, erişim tarihi Haziran 3, 2026, https://d-nb.info/1365970787/34 35.An Urgent Matter of Drones: Lessons for NATO from Ukraine - CEPA, erişim tarihi Haziran 3, 2026, https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/ 36.Dispersed, Disguised, and Degradable: The Implications of the Fighting in Ukraine for Future U.S.-Involved Conflicts - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf 37.Project Maven - Wikipedia, erişim tarihi Haziran 3, 2026, https://en.wikipedia.org/wiki/Project_Maven 38.US used AI to find targets for strikes on Syria and Yemen - The National News, erişim tarihi Haziran 3, 2026, https://www.thenationalnews.com/world/us-news/2024/02/26/us-ai-syria-yemen/

39.The Unmanned Space: How Autonomous Systems Are Transforming Defense Operations,

erişim tarihi Haziran 3, 2026, https://www.atlas-tech.com/the-unmanned-space-how-autonomous-systems-are-transforming-defense-operations/ 40.Pentagon IG moves to assess high-stakes Replicator initiative | DefenseScoop, erişim tarihi Haziran 3, 2026, https://defensescoop.com/2024/07/29/pentagon-inspector-general-assessment-replicator-initiative-memo/

41.: Integrated Deterrence and US Defense Strategy in NATO and AUKUS: An Analysis of Advanced Technologies and Multi-Domain Operati - Department of War, erişim tarihi Haziran 3, 2026, https://media.defense.gov/2025/Sep/25/2003808532/-1/-1/1/GLOBAL%20-%20D OLAN%20-%20DISCLAIMER.PDF 42.Calibrating NATO's Vision of AI-Enabled Decision Support - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support

43.Stop Saying "AI" - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2602.17729 44.How NATO can integrate AI to prevail in future algorithmic warfare - Atlantic Council, erişim tarihi Haziran 3, 2026, https://www.atlanticcouncil.org/in-depth-research-reports/report/how-nato-can-integrate-ai-to-prevail-in-future-algorithmic-warfare/ 45.How Artificial Intelligence Could Reshape Four Essential Competitions in Future Warfare - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA4300/RRA431 6-1/RAND_RRA4316-1.pdf 46.Autonomous and automated weapon systems and the traditional dynamics of conflict escalation. | Future Forge, erişim tarihi Haziran 3, 2026, https://theforge.defence.gov.au/article/autonomous-and-automated-weapon-syste ms-and-traditional-dynamics-conflict-escalation 47.Artificial Intelligence in Modern Warfare - Army University Press, erişim tarihi Haziran 3, 2026, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2024/Artificial-Intelligence-Strategic-Innovation-and-Emergi ng-Risks/ 48.NATO needs a 'hellscape' defense at 'Replicator' speed - Atlantic Council, erişim tarihi

Haziran 3, 2026,

https://www.atlanticcouncil.org/in-depth-research-reports/report/nato-needs-a-hellscape-defense-at-replicator-speed/ Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken otonom hedefleme ve DSS yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası hız-doğruluk dengesi, hukuki filtre, anlamlı insan kontrolü ve sorumluluk üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle otonom hedefleme ve DSS alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler

de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● ● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Otonom Hedefleme ve Karar Destek Sistemleri alanında en güçlü erken uyarı göstergeleri
hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

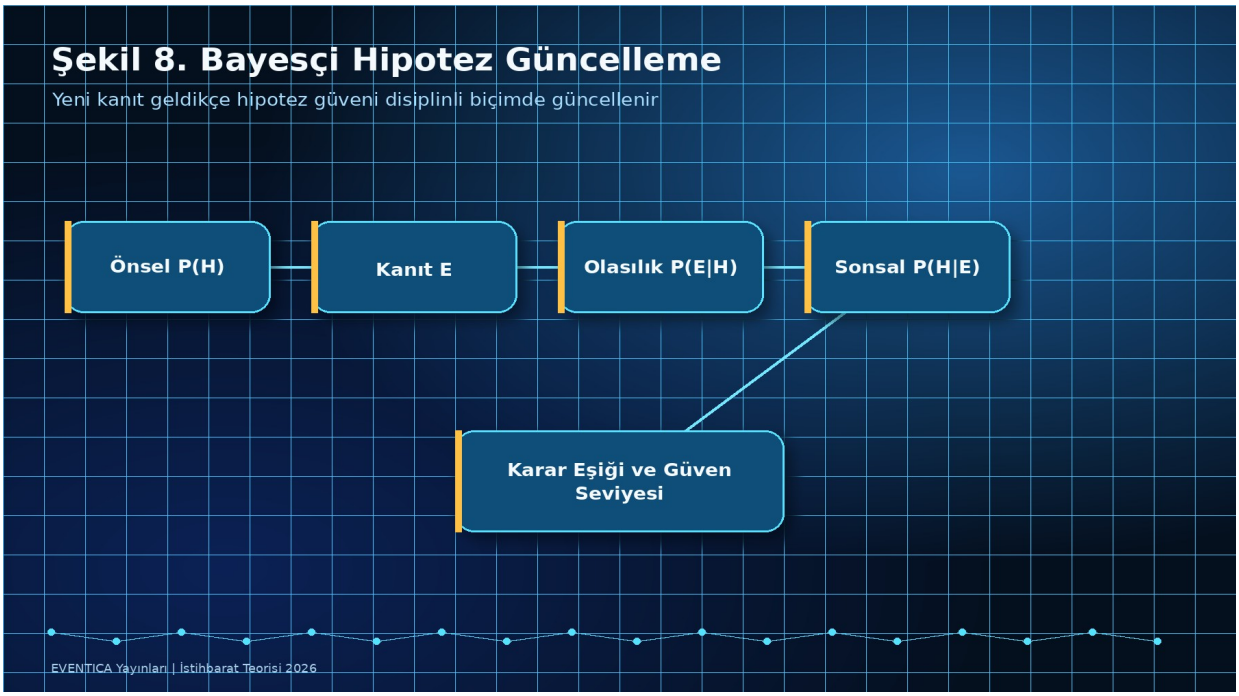
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 8. Bayesçi İstihbarat: Kanıt, Olasılık ve Hipotez Güncelleme

Bayes bu kitapta ayrı bir bölüm olarak korunmuştur. Temel formül: P(H|E) = [P(E|H) × P(H)] / P(E). Bu formül, yeni kanıt geldikçe hipotez güveninin nasıl güncelleneceğini gösterir.



Şekil 8. Bayesçi hipotez güncelleme döngüsü

Tablo 11. Bayes formülünün istihbarattaki karşılığı

Matematiksel öğe	İstihbarat karşılığı	Pratik soru
P(H)	Önsel hipotez olasılığı	Bu aktör geçmişte ne yaptı, kapasitesi ne?
P(E|H)	Hipotez doğruysa kanıtı görme olasılığı	Bu kanıt beklenen bir emare mi?
P(E)	Kanıtın genel görülme olasılığı	Bu sinyal sıradan mı, ayırt edici mi?
P(H|E)	Güncellenmiş olasılık	Yeni kanıt hipotezi ne kadar güçlendirdi?

1. Kavramsal Çerçeve

İstihbarat analizi çoğu zaman kesinlik üretmez; daha dürüst bir ifadeyle belirsizliği yönetir. Bir analistin elindeki veri hiçbir zaman tam değildir. Kaynaklar eksik olabilir, sensörler yanılabilir, sosyal medya verisi manipüle edilebilir, insan kaynakları bilerek

veya bilmeden yanlış aktarım yapabilir. Bu yüzden iyi analiz, “kesin böyledir” demekten önce, eldeki kanıtın hangi hipotezi ne kadar güçlendirdiğini hesaplamaya çalışır. Bayesçi düşünme tam burada devreye girer.

Bayes formülü, yeni bir kanıt geldiğinde bir hipoteze duyulan inancın nasıl güncellenmesi gerektiğini gösteren temel olasılık modelidir:

P(H|E) = [P(E|H) × P(H)] / P(E)

Burada H hipotezi, E ise yeni kanıtı ifade eder. P(H), kanıt gelmeden önce hipoteze verilen önsel olasılıktır. P(E|H), hipotez doğruysa bu kanıtı görme olasılığıdır. P(E), kanıtın genel

görülme olasılığıdır. P(H|E) ise kanıt geldikten sonra hipotezin güncellenmiş, yani sonsal

olasılığıdır. Bu formül istihbaratta sadece matematiksel bir süs değildir. Asıl değeri, analistin zihnindeki belirsizliği disipline etmesidir. Çünkü istihbarat hatalarının önemli bir kısmı veri eksikliğinden değil, kanıtın ağırlığını yanlış okumaktan çıkar. Bir kanıt yeni olabilir ama zayıf olabilir. Bir kaynak güvenilir görünebilir ama bağlam dışı aktarım yapmış olabilir. Bir gösterge sık görülüyor olabilir ama hedef olayla nedensel bağı zayıf olabilir. Bayesçi çerçeve bu karmaşayı daha açık hale getirir.

2. İstihbarat Döngüsünde Bayesçi Güncelleme

Bayesçi istihbarat yaklaşımı dört aşamalı işler. İlk aşama hipotez kurmaktır. Örneğin “aktör X yakın vadede siber ön-konumlanma yapıyor” gibi bir hipotez belirlenir. İkinci aşama önsel olasılığı tanımlamaktır. Bu olasılık geçmiş davranış, kapasite, niyet, coğrafi bağlam, teknik imkan ve önceki emarelerden çıkarılır. Üçüncü aşama yeni kanıtın ağırlığını ölçmektir. Yeni kanıt hipotez doğruysa gerçekten beklenen bir şey mi, yoksa başka hipotezlerle de açıklanabilir mi? Dördüncü aşama karar eşiğidir. Güncellenmiş olasılık hangi seviyeye çıktığında uyarı, izleme, diplomatik temas, savunma hazırlığı veya operasyonel aksiyon önerilecektir?

Burada kritik nokta şudur: Bayesçi analiz analistin yerine karar vermez. Analistin kanıtı daha temiz tartmasını sağlar. Yani sistem “bu kesin tehdittir” demez; “bu kanıt, şu hipotezi önceki duruma göre şu kadar güçlendirdi” der. Bu fark çok önemlidir. Çünkü modern istihbaratta karar vericiye verilen güven seviyesi, analizin kendisi kadar değerlidir.

3. Kaynak Güvenilirliği ve Kanıt Ağırlığı

Bayesçi çerçevede her kanıt aynı değerde değildir. Bir uydu görüntüsü, sosyal medya paylaşımı, HUMINT raporu, siber gösterge, ticari veri seti veya açık kaynak haber aynı hipotezi destekliyor gibi görünebilir. Fakat bunların güvenilirliği, güncelliği, manipülasyona açıklığı ve

bağlamsal uyumu farklıdır. Bu nedenle Bayesçi modelde kaynak güvenilirliği ayrı bir ağırlık olarak ele alınmalıdır. Pratikte üç soru sorulur. Birincisi: Kanıt doğru mu? İkincisi: Kanıt hipotezle gerçekten ilişkili mi? Üçüncüsü: Bu kanıt başka hangi hipotezlerle de açıklanabilir? Üçüncü soru genellikle en fazla ihmal edilen sorudur. Çünkü analistler çoğu zaman kendi ana hipotezlerini destekleyen kanıtları daha hızlı kabul eder. Bu da doğrulama yanlılığına yol açar.

Bayesçi yaklaşım bu yanlılığı kırar. Eğer bir kanıt hem H1 hipoteziyle hem de H2 hipoteziyle açıklanabiliyorsa, kanıtın ayırt edici gücü düşer. İstihbarat açısından değerli kanıt, sadece doğru olan değil, rakip hipotezleri birbirinden ayırabilen kanıttır.

4. Yanlış Pozitif, Yanlış Negatif ve Alarm Yönetimi

İstihbarat sistemlerinde en tehlikeli iki hata türü yanlış pozitif ve yanlış negatiftir. Yanlış pozitif, tehdit olmadığı halde tehdit varmış gibi alarm üretmektir. Yanlış negatif ise tehdit varken bunu kaçırmaktır. Modern veri akışlarının büyüklüğü bu iki hatayı da

büyütür. Çok hassas bir sistem sürekli alarm üretir ve analist yorgunluğu yaratır. Çok katı bir sistem ise kritik sinyalleri kaçırabilir.

Bayesçi karar eşiği bu yüzden önemlidir. Her kurum, her tehdit tipi için aynı eşikle çalışamaz. Kritik altyapı savunmasında düşük olasılıklı ama yüksek etkili riskler daha erken alarm gerektirir. Diplomatik kriz analizinde ise yanlış alarmın maliyeti daha yüksek olabilir. Bu nedenle istihbarat analizinde olasılık tek başına yetmez; olasılık, etki ve karar maliyeti birlikte okunmalıdır.

5. Bayesçi Füzyon: Çok Kaynaklı İstihbaratta Kullanım

Çağdaş istihbarat artık tek kaynağa yaslanmaz. OSINT, SIGINT, GEOINT, HUMINT, CTI, finansal göstergeler, ticari veri akışları ve sosyal medya sinyalleri aynı analiz alanına girer. Bu kaynakların her biri hipotez üzerinde küçük veya büyük güncellemeler yaratır. Bayesçi füzyonun gücü burada ortaya çıkar: farklı kaynaklardan gelen kanıtlar tek tek değil, birbirleriyle ilişkili biçimde tartılır.

Ancak burada basit bir toplama yapılmaz. Çünkü kaynaklar bağımsız olmayabilir. Bir haber, başka bir haberden kopyalanmış olabilir. Bir sosyal medya dalgası bot ağları tarafından şişirilmiş olabilir. Bir teknik gösterge aynı altyapıdan türemiş olabilir. Bu nedenle Bayesçi analizde bağımsızlık varsayımı dikkatle test edilmelidir. Aynı kökten gelen üç kanıt, gerçekten üç ayrı kanıt değildir; aynı kanıtın üç farklı yüzüdür.

6. Bayes ve Yapay Zekâ Destekli Analiz

Yapay zekâ destekli istihbarat sistemleri büyük veri setlerini hızla işler; fakat bu hız her zaman epistemik güvenilirlik anlamına gelmez. Model güçlü bir örüntü bulabilir ama bu örüntünün hangi hipotezi ne kadar desteklediğini açıkça söylemeyebilir. Bayesçi çerçeve, yapay zekâ çıktılarının karar vericiye daha anlaşılır aktarılmasını sağlar.

Örneğin bir model “risk yüksek” dediğinde bu ifade tek başına yetersizdir. Daha doğru çıktı şuna benzer olmalıdır: “Önsel risk orta seviyedeydi. Yeni teknik gösterge, kaynak güvenilirliği ve benzer olay geçmişi dikkate alındığında hipotezin olasılığı arttı. Ancak kanıtın bağımsızlığı sınırlı olduğu için güven seviyesi orta-yüksek olarak değerlendirilmelidir.” Bu tarz bir çıktı hem analitik hem de yönetsel olarak daha değerlidir.

7. Bayesçi Düşünmenin Sınırları

Bayes güçlüdür ama sihirli değildir. Önsel olasılıklar yanlış kurulursa sonuç da yanlış yönde güncellenir. Kaynak bağımsızlığı yanlış varsayılırsa model aşırı güven üretir. Nadir olaylarda veri az olduğu için olasılık tahminleri kırılgan hale gelir. Ayrıca siyasi baskı, kurum kültürü ve kriz psikolojisi gibi faktörler matematiksel modelin dışında kalabilir.

Bu yüzden Bayesçi analiz, insan muhakemesinin yerine değil, yanına konmalıdır. En iyi kullanım biçimi şudur: hipotezleri görünür hale getir, önsel varsayımları açık yaz, kanıtın gücünü tart, rakip hipotezleri zorla, güncellenmiş olasılığı karar eşiğiyle bağla ve sonucu güven seviyesiyle birlikte sun.

8. İstihbarat Ürünü Formatı

Bayesçi yaklaşım, final istihbarat ürününe de yansıtılmalıdır. Her ciddi analiz notunda şu alanlar bulunabilir: ana hipotez, rakip hipotezler, önsel değerlendirme, yeni kanıtlar, kaynak güvenilirliği, kanıt bağımsızlığı, güncellenmiş olasılık, güven seviyesi, karar eşiği ve önerilen izleme göstergeleri. Bu format analizin hesabını verilebilir hale getirir.

Sonuç olarak Bayes formülü, istihbaratta sadece olasılık hesabı değildir. Bir disiplin biçimidir.

Analisti daha açık düşünmeye, karar vericiyi daha doğru bilgilendirmeye ve kurumu daha ölçülebilir bir karar mimarisine taşır. 2026 sonrası istihbarat teorisinde Bayesçi muhakeme, yapay zekâ destekli sistemlerin güvenilirliği ve insan-makine karar ortaklığı için temel bir kolon olarak görülmelidir.

Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken Bayesçi istihbarat yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası önsel olasılık, kanıt ağırlığı, kaynak güvenilirliği ve karar eşiği üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle Bayesçi istihbarat alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● ● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Bayesçi İstihbarat: Kanıt, Olasılık ve Hipotez Güncelleme alanında en güçlü erken uyarı
göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

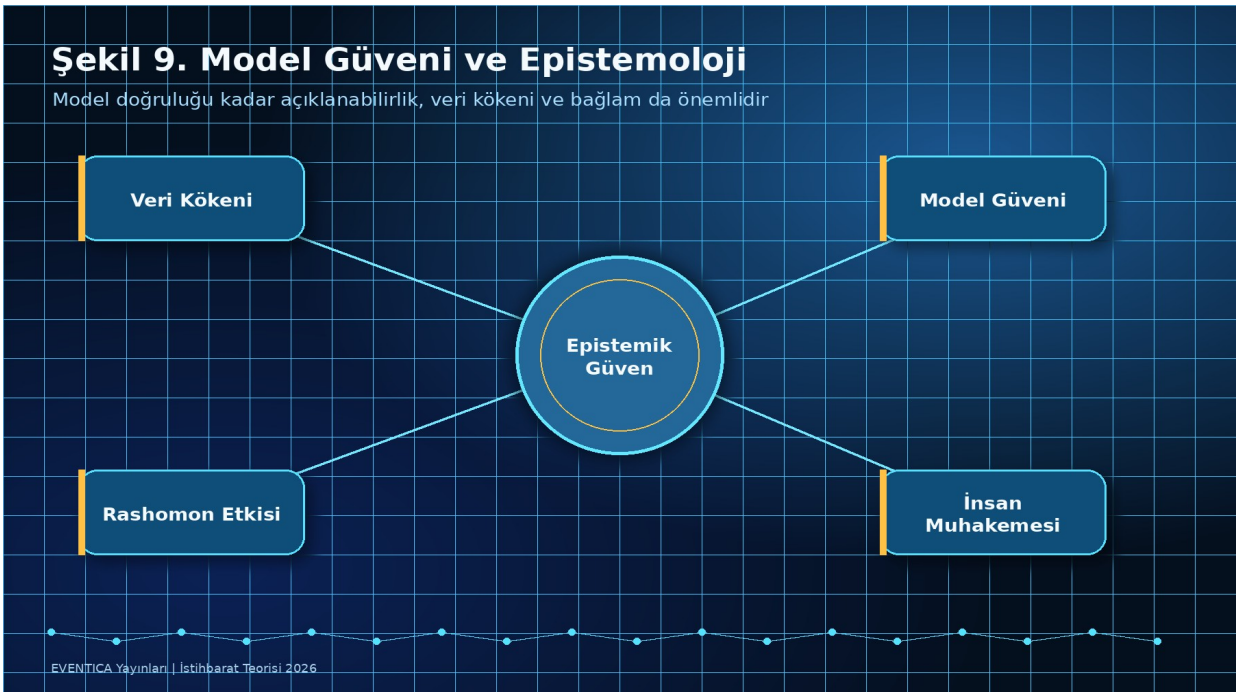
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030'a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 9. Makine Öğrenmesinin İstihbari Epistemolojisi

Makine öğrenmesi daha fazla cevap üretir; ama cevapların hangisinin doğru, uygulanabilir ve bağlama uygun olduğunu ayrıca test etmek gerekir.



Şekil 9. Makine öğrenmesi kaynaklı epistemolojik risk hattı

Tablo 12. Epistemolojik patolojiler

Patoloji	Kısa tanım	İstihbarat riski
Analiz felci	Çok veri ve çok seçenek nedeniyle kararın gecikmesi	Eyleme dönüşmeyen ürün
Uygulanamaz çözümler	Laboratuvarda iyi, sahada zayıf model çıktısı	Operasyonel kopukluk
Rashomon etkisi	Aynı veriyi açıklayan çok sayıda model	Güven krizleri
Otomasyon yanlılığı	Makine çıktısına gereğinden fazla güven	İnsan muhakemesinin zayıflaması

Tablo 12. Epistemolojik patolojiler
Patoloji

Kısa tanım İstihbarat riski Analiz felci Çok veri ve çok seçenek nedeniyle kararın gecikmesi Eyleme dönüşmeyen ürün Uygulanamaz çözümler Laboratuvarda iyi, sahada zayıf model çıktısı Operasyonel kopukluk Rashomon etkisi Aynı veriyi açıklayan çok sayıda model Güven krizleri Otomasyon yanlılığı Makine çıktısına gereğinden fazla güven İnsan muhakemesinin zayıflaması Makine Öğrenmesinin İstihbari Epistemolojisi: Analiz Felci, Uygulanamaz Çözümler ve

Algoritmik Rashomon Etkisi

1. Kavramsal Çerçeve İstihbarat analizi, en temel formunda epistemolojik bir faaliyettir;

bilginin doğasını, kaynağını, sınırlarını ve geçerliliğini sorgulama pratiğidir. Geleneksel istihbarat teorisi, gerçekliğin ontolojik varsayımlarından ziyade, "neyi nasıl bildiğimizi" anlamaya yönelik epistemolojik çabalar etrafında şekillenir.1 İstihbarat uygulayıcıları ve stratejik karar vericiler için bilginin kriteri tarihsel olarak her zaman pragmatik olmuştur. "En iyi gerçek", "işe yarayan şey" ve benzeri ifadeler, bilginin yararlılık ilkesi üzerinden değerlendirildiğini varsayar; zira postmodern felsefenin "gerçeklik yoktur, sadece yarışan

anlatılar vardır" şeklindeki varsayımları, sahada hayati kararlar alması gereken bir istihbarat analisti için hiçbir operasyonel değer taşımaz.1 Ne var ki, dijital çağın sunduğu devasa Açık Kaynak İstihbaratı (OSINT) havuzları, kesintisiz Bilgi, Gözetleme ve Keşif (ISR) veri akışları ve bu verileri işlemek üzere tasarlanan Makine Öğrenmesi (ML) ile Yapay Zekâ (AI) sistemleri, bilginin üretilme ve doğrulanma biçiminde köklü bir kriz yaratmıştır. İstihbarat toplulukları, insan merkezli analizden, insan-makine ekosistemine doğru kayarken, algoritmaların ürettiği bilginin epistemolojik doğası üç temel patoloji etrafında düğümlenmektedir: Analiz felci (analysis paralysis), uygulanamaz çözümler (inapplicable solutions) ve algoritmik Rashomon etkisi.

Birinci patoloji olan analiz felci, modern savaş alanındaki sensörlerin ve veri toplayıcıların neredeyse her yerde hazır bulunmasıyla başlayan aşırı enformasyon yüklemesinin bir sonucudur.2 Algoritmalar, insanın bilişsel sınırlarını aşan devasa veri setlerini saniyeler içinde işleyerek sayısız içgörü üretebilmektedir; ancak bu bolluk, karar alma sürecini hızlandırmak yerine yavaşlatma veya tamamen durdurma riski taşır.2 Barry Schwartz'ın psikoloji literatürüne kazandırdığı "seçenek paradoksu" (paradox of choice) kavramı, istihbarat sahasında karar alıcıların sonsuz analitik spesifikasyon ve değişken karşısında yanlış karar verme korkusu yaşayarak eylemsizliğe itilmesi şeklinde tezahür eder.4 İstihbarat döngüsünün hızı, verinin hacmi altında ezilmekte, eyleme dönüştürülemeyen "teorik" istihbarat yığınları oluşmaktadır.

İkinci patoloji olan uygulanamaz çözümler, algoritmaların laboratuvar ortamında sergiledikleri yüksek istatistiksel başarının, savaşın ve insan doğasının doğrusal olmayan (non-linear), kaotik açık sistemlerinde 1 işlevsiz kalması durumudur. Savaş, Carl von Clausewitz'in altını çizdiği gibi, sürtünme (friction), şans ve tepki veren canlı iradelerin etkileşimiyle şekillenir.5 Makine öğrenmesi ise istatistiksel olasılıklar ve tümevarımsal (inductive) kurallar üzerinden işler.5 Modeller, "sinyal" (anlamlı ve sistematik aktivite örüntüsü) ile "gürültüyü" (beklenmedik hava olayları, şans, iletişim kopuklukları) birbirinden ayırmakta zorlandıklarında, aşırı uyum (overfitting) sorunu ortaya çıkar.4 ChatGPT veya Claude gibi Büyük Dil Modelleri (LLM) insan zekasını etkileyici bir şekilde taklit etseler de, veriyi bir insanın anladığı tarihsel ve duygusal bağlamda "anlamazlar".7 Bu epistemolojik boşluk, makinenin istatistiksel korelasyonu nedensellik zannetmesine ve sonuçta askeri veya politik bir operasyona entegre edilemeyen, gerçek dünya koşullarına yabancı "uygulanamaz" çözümler üretmesine neden olur.9 Üçüncü ve en derin felsefi sarsıntı ise algoritmik Rashomon etkisidir. İsim, Akira Kurosawa'nın aynı cinayet olayını farklı ve birbiriyle çelişen ama kendi içinde son derece tutarlı perspektiflerden anlatan

karakterleri konu alan 1950 yapımı meşhur filminden ödünç alınmıştır.10 Makine öğrenmesi bağlamında Leo Breiman tarafından literatüre entegre edilen bu terim, aynı veri seti üzerinde eğitilmiş ve yaklaşık olarak aynı yüksek hata/başarı oranına sahip

olan ancak veriyi açıklarken tamamen farklı değişkenlere bel bağlayan çok sayıda "iyi" modelin aynı anda var olabilmesi fenomenini açıklar.10 İstihbarat analisti için bu durum, kestirimsel çokluluk (predictive multiplicity) krizini doğurur.13 Bir bireyin veya hedefin risk profilini değerlendiren iki farklı algoritma, aynı matematiksel başarı düzeyine sahip olmalarına rağmen birbirine tamamen zıt sonuçlar verebilmektedir. Böyle bir ortamda "gerçek", tekil bir analitik çıktı olmaktan çıkıp, veri setinin ve algoritma tasarımcısının prosedürel seçimlerinin rastgele bir tezahürü haline gelir.

Patoloji Türü Epistemolojik Krizin Karar Alıcılar Üzerindeki Doğası Taktik ve Stratejik Etkisi Analiz Felci Enformasyonun niceliğinin, Zamanında karar insan zihninin niteliksel verememe, eylemsizlik, sentez kapasitesini aşması. artan belirsizlik, sistemler arası kredibilite itilafı.2 Uygulanamaz Çözümler İstatistiksel tümevarımın Savaşın açık sistem bağlamsal nedensellik doğasına uymayan, zannedilmesi, dışsal laboratuvar değişkenlerin yok sayılması.

mükemmelliğinde ama sahada kör olan planlar.1 Rashomon Etkisi "Tek bir doğru model" Kestirimsel keyfilik, güven varsayımının çökmesi;

eşit kaybı, sistem çıktılarının derecede geçerli ama zıt yasal/ahlaki izlenebilirliğinin önerilerin varlığı. (XAI) imkânsızlaşması.11

2. Akademik Teoriler Makine öğrenmesinin karar destek mekanizmalarına ve istihbarat

pratiklerine entegrasyonu, salt bir mühendislik meselesi değil, veri bilimi, psikoloji, askeri strateji ve felsefenin kesişiminde yer alan derin bir teorik problemdir. Akademik literatür, insan ve makine zekasının bu sancılı entegrasyonunu anlamlandırmak için çeşitli çerçeveler sunmaktadır.

2.1. İki Kültür Paradigması ve Rashomon Kümelerinin Matematiği

İstatistik ve veri bilimi dünyasında devrim yaratan Leo Breiman'ın 2001 tarihli "İki Kültür" (Two Cultures) makalesi, günümüz algoritmik istihbarat krizlerinin felsefi temelini oluşturur.

Breiman, veriyi anlamlandırmada iki zıt kültür tanımlamıştır: Veriyi üreten mekanizmayı doğrusal ve anlaşılır bir şekilde modellemeye çalışan geleneksel "istatistiksel" yaklaşım ve doğadaki gerçek süreci temsil etme kaygısı gütmeden doğrudan veriye uyan tahminsel "algoritmik" yaklaşım (örneğin rastgele ormanlar veya derin sinir ağları).16 Algoritmik

modeller, veriyi üreten sürecin nedenselliğini temsil etmek üzere tasarlanmamıştır; yalnızca örüntü tanımaya odaklanırlar. Bu ayrım, algoritmik modellerin doğası gereği neden açıklanabilirlikten (explainability) uzak olduğunu ve Rashomon etkisine neden zemin hazırladığını açıklar.16 Rashomon etkisi teorik olarak, tahmin görevlerinin (özellikle bireysel riskler veya askeri eylemler gibi gürültülü süreçlerin) birden fazla, benzer derecede isabetli model kabul etmesi durumudur.15 Matematiksel ve yapısal olarak bir "Rashomon Kümesi" (Rashomon Set), belirli bir ε tolerans seviyesi içinde en iyi performans gösteren modelle yaklaşık olarak aynı genelleme performansına sahip tüm modellerin kümesi olarak ifade edilir:

$$R_\varepsilon = \{ f \in F \mid L(f) \leq L(f^*) + \varepsilon \}$$

Burada F aday model ailesini, f* en düşük hata/kayıp değerine sahip referans modeli, L(f) ilgilenilen modelin hata oranını veya kayıp değerini, ε ise kabul edilebilir performans toleransını temsil eder. Bu tanım, aynı veri seti üzerinde birbirinden farklı fakat benzer derecede başarılı çok sayıda modelin bulunabileceğini gösterir.

Fisher, Rudin ve Dominici'nin (2019) çalışmalarında vurguladığı üzere, bu etki özellik önemi (feature importance) atıflarının güvenilirliğini derinden sarsar.12 Şartlı tahliye, sağlık, finans ve ulusal güvenlik gibi yüksek riskli (high-stakes) kararlarda kullanılan ve gürültülü (nondeterministic) süreçlerden elde edilen veriler, devasa Rashomon kümeleri oluşturmaya meyillidir.17 Başka bir deyişle, hedef belirlemede kullanılan bir

makine öğrenmesi sistemi size bir "gerçek" sunduğunda, aslında matematiksel olarak aynı geçerliliğe sahip ama tamamen farklı değişkenlere (örneğin bir bireyin iletişim frekansından ziyade coğrafi konumuna) odaklanan sayısız başka "gerçek" model daha perde arkasında varlığını sürdürmektedir.11

2.2. Sinyal, Gürültü ve İstatistiksel Belirsizliğin Epistemolojisi

İstihbarat teşkillerinin makine öğrenmesini operasyonelleştirmesindeki teorik zorluk, modelin ölçtüğü şeyin "ne olduğu" sorusudur. Öngörüsel modellemede, sistemler "sonuç" (outcome) ile "yordayıcılar" (predictors) arasındaki ilişkiyi tespit etmeye çalışır.4 Bu ilişki incelenirken "sinyal", makine öğrenmesi algoritmalarının odaklandığı, düşmanın askeri becerisi, iradesi, organizasyonu ve liderliği gibi anlamlı etkinlik örüntüleridir.4 Buna karşın "gürültü", iletişim kopuklukları, hava muhalefeti, bireysel hata gibi tahmin edilebilirliği bozan rastgele unsurlardır.4 Akademik açıdan bakıldığında, yapay zekânın "makine epistemolojisi" üretip üretemeyeceği, zihne veya bilinçli deneyimlere sahip olup olmadığı tartışmalıdır.18 Sembol manipülasyonu olmaksızın makine zekasının insan ahlakını anlayıp anlayamayacağı sorusu, Barry Smith gibi filozoflar tarafından duyguların ontolojisi (ontology of emotions) bağlamında incelenmektedir.18 İnsan hislerini, korkularını veya Clausewitz'in deyimiyle savaşan bir ordunun "canlı iradesini" 5 sayılara dökmek kaçınılmaz olarak yapay bir dayatmadır.19

Dolayısıyla, veri modelleri gürültüyü sinyal sanarak "aşırı uyum" (overfitting) gösterdiğinde 6 veya "karıştırıcı değişkenleri" (confounding variables) kontrol etmeyi başaramadığında (örneğin bir ordunun başarısını sadece teknolojiye bağlayıp ekonomik gelişmişliği göz ardı etmek gibi), ortaya çıkan istihbarat yapısal olarak kusurlu hale gelir.4

2.3. Bilişsel Sınırlılıklar: Otomasyon Yanlılığı ve Algoritma Tiksintisi

İnsan zihninin yapay zekâ sistemleriyle girdiği etkileşim, davranışsal bilimler ve psikoloji ekseninde iki zıt kutupta incelenir. Karar destek sistemlerinin inşasında bu bilişsel önyargıların anlaşılması hayati önem taşır.20 Bir yanda otomasyon yanlılığı (automation bias) bulunur. Bu eğilim, insan operatörlerin algoritmik sistemlerin çıktılarına aşırı güvenmesi, onları insan yargısından daha nesnel ve hatasız kabul etmesi durumudur.3 Özellikle düşük uzmanlık seviyesindeki veya yeni sistemlere aşina olmayan kullanıcılar, "algoritmik duyarlılık" (algorithmic susceptibility) göstererek makine tavsiyelerini yüksek oranda sorgusuz sualsiz kabul ederler.21 Ancak otomasyon yanlılığı sadece acemilere özgü değildir; OODA (Gözlem, Yönelim, Karar, Eylem) döngüsünün olağanüstü hızlandığı, zaman baskısı ve bilgi yoğunluğunun arttığı durumlarda deneyimli analistler dahi kendi yargılarını askıya alarak makinelerin direktiflerine rıza gösterme eğilimine girerler.24 Bu durum ahlaki körelmeye (moral deskilling) ve makinenin hatalarının sistemik felaketlere dönüşmesine yol açar.26 Diğer yanda ise algoritma tiksintisi (algorithm aversion) yer almaktadır. Yüksek uzmanlığa sahip analistler ve deneyimli askeri personel, başlangıçta algoritmik tavsiyeleri reddetme ve kendi içgüdülerine güvenme eğilimindedir.21 Görev aşinalığı (task familiarity) yüksek olan kullanıcılar, yapay zekâ sistemlerine daha az bağlılık gösterdiklerini beyan etseler de, karmaşık görevler sırasında ironik bir biçimde yapay zekâya yine de aşırı güvendikleri (over-trust) vakalarla sabittir.21 İlginç bir şekilde, West Point askeri öğrencileri (cadets) üzerinde yapılan ampirik bir deney, askeri eğitim almış bireylerin genel kamuoyuna kıyasla otomasyon yanlılığına daha az yatkın olduğunu ve algoritmik karar destek sistemlerine karşı çok daha "kalibre edilmiş bir güven" (calibrated trust) sergilediklerini ortaya koymuştur.22

Psikolojik Eğilim Tetikleyici Faktörler İstihbari Karar Sürecindeki Etkisi

Otomasyon Yanlılığı Düşük uzmanlık, zaman Hatalı kararların baskısı, yorgunluk, hesap meşrulaştırılması, analistin verebilirlik eksikliği.21 sistemi onaylayan (rubber-stamp) bir robota dönüşmesi.3

Algoritma Tiksintisi Yüksek uzmanlık ve görev Geçerli algoritmik aşinalığı, sistemin kara kutu öngörülerin reddedilmesi, (black box) doğası.21 sistemin entegrasyonunun

organizasyon içinde dirençle karşılaşması.21 Bilişsel Aşırı Yük Devasa veri akışı, çelişen AI Seçenek paradoksu, kararın risk skorları, Rashomon ertelenmesi, analiz felci.2 kümeleri.3

3. Sistem Mimarisi İstihbarat toplulukları ve savunma organizasyonları için salt "daha akıllı"

algoritmalar inşa etmek, analiz felci ve uygulanamaz çözümler sorununu ortadan kaldırmaz. Bunun yerine, Sosyal ve Davranışsal Bilimlerin (SBS) rehberliğinde şekillenen, donanım, yazılım ve insan operatörleri içeren kapsamlı bir "İnsan-Makine Ekosistemi" (Human-Machine Ecosystem) mimarisi tasarlanmalıdır.20

3.1. Hibrit Veri Hattı (Pipeline) ve Triyaj Mantığı

Devasa veri okyanusunda boğulmayı (drowning in data) engellemenin yegâne yolu hibrit iş akışlarıdır. Modern İstihbarat, Gözetleme ve Keşif (ISR) sistemlerinde verinin toplanma hızı ile insanın bu veriyi doğrulama hızı arasında oluşan uçurum (velocity mismatch), analiz felcinin yapısal kökenidir.3 Bunu aşmak için tasarlanan AI mimarisi, yapay zekâyı karar verici değil, bir filtre ve triyaj mekanizması olarak konumlandırmalıdır.3 Bu mimaride süreç şu şekilde işler:

Açık kaynaklardan (OSINT), uydulardan ve sensörlerden gelen ham veri selini ilk olarak makine öğrenmesi modelleri karşılar.2 AI, anormallikleri tespit eder, kaynakları birbiriyle ilişkilendirir ve veriyi önceliklendirir.3 Önceden ayarlanmış matematiksel "ilgililik eşiklerini" (relevance thresholds) aşmayan tüm rutin veriler sistem tarafından arşivlenirken, yalnızca bu eşikleri aşan yüksek öncelikli tehdit uyarıları insan analistlerin ekranına düşer.3 Eğer sistem analistin inceleyebileceğinden daha az öğe döndürürse analist verimsiz kalır; çok fazla döndürürse analiz felci başlar.30 Bu nedenle kapasiteye uygun optimal eşik optimizasyonu (threshold optimization), sistem mimarisinin kalbini oluşturur.30 Böylelikle hedefleme, stratejik analiz ve kuvvet kullanımı gibi yüksek sonuçlu yargılarda nihai karar yetkisi insanda kalmaya devam eder.3

3.2. Açıklanabilir Yapay Zekâ (XAI) ve IEMA Çerçevesi

Makine öğrenmesi modellerinin iç mantığını açıklayamaması (kara kutu problemi), istihbarat analizinde "uygulanamaz çözümler" patolojisinin ana kaynağıdır.7 ABD Savunma Bakanlığı (DoD) ve RAND Corporation gibi kurumların stratejik araştırmaları, XAI (Açıklanabilir Yapay Zekâ) mimarilerinin geliştirilmesini ulusal güvenlik vizyonunun merkezine

koymaktadır.32 Ancak klasik açıklanabilirlik metotları modelin sadece bir yönüne odaklanarak yanıltıcı olabilmektedir.36 Bunun yerine, "Etkileşimli Açıklayıcı Model Analizi" (Interactive Explanatory Model Analysis - IEMA) gibi mimariler benimsenmektedir. IEMA, bilişsel bilimlerden aldığı ilhamla, analist ile model arasında statik değil, sıralı ve etkileşimli bir diyalog grameri oluşturur.36 Analist, modelin karar sürecindeki ağırlıkları manuel olarak değiştirip test ederek algoritmik duyarlılık analizi yapabilir.

Model seçimi bağlamında tasarımcılar, doğruluk oranı ile yorumlanabilirlik arasındaki dengeyi "Rashomon Dirseği" (Rashomon elbow) üzerinden kurgulamalıdır. Rashomon eğrisinde bu dirsek noktası, sistemin gereksiz karmaşıklıktan kurtulup daha basit ve şeffaf hale gelirken aynı zamanda yüksek isabet oranını (low empirical risk) koruduğu ideal tasarım bölgesini temsil eder.37 Savaş ortamı gibi gürültülü (noisy) veri setlerinde, doğası gereği yorumlanabilir (inherently interpretable) modellere her zaman öncelik verilmelidir.17

3.3. Düşmanca Eğilimlere Dirençli Mimariler ve NATO Standartları

Karar destek sistemleri, sivil hayattaki benzerlerinin aksine, düşmanın bilinçli manipülasyonuna maruz kalır.3 Bir hasım, sensör verilerini zehirleyerek (data poisoning) veya görsel imzalarını makine tespit eşiklerinin altına çekerek yapay zekâ mimarisini kasıtlı olarak yanıltabilir.3 Buna karşı savunma algoritmaları, "Gürültüye

Dirençli Regresyon" (Noise Resilient Regression) ve "Düşmanca Etkilere Dirençli Regresyon" (Adversarial-resilient regression) mimarileri şeklinde iki kategoriye ayrılır; temel mantık, sisteme sızan aykırı değerleri (outliers) tespit edip silmek üzerine kuruludur.38 NATO'nun yapay zekâ vizyonu incelendiğinde, karar destek mimarilerinde en büyük engellerden birinin sistemler arası "birlikte çalışabilirlik" (interoperability) olduğu görülmektedir.39 Veri kalitesi, model eğitimi ve mansap (downstream) model performansı arasındaki uyumsuzluk, ittifak üyelerinin kullandığı farklı algoritmaların eski veya ilgisiz veri üzerinden uyuşmayan değerlendirmeler yapmasına yol açar.39 Kesintisiz entegrasyon sağlanamazsa, AI sistemlerinin yaratacağı "akıllı" destek, yerini karargahlar arası "bilişsel kaosa" bırakır.

4. Gerçek Dünya Vakaları

Akademik literatürdeki epistemolojik problemler (Rashomon etkisi, analiz felci ve uygulanamaz çözümler), doğrudan çatışma alanlarında ve adli bilişim pratiklerinde dramatik ve somut sonuçlar doğurmuştur.

4.1. İsrail'in Gazze'deki AI Destekli Hedefleme Sistemleri: Lavender ve The

Gospel

Ekim 2023 sonrasında şiddetlenen İsrail-Hamas çatışması, yapay zekânın ölümcül karar destek süreçlerinde kullanılmasının (AI DSS) tarihsel bir test sahası olmuştur. İsrail Savunma Kuvvetleri (IDF), istihbarat analistlerine hedef tavsiyeleri sunmak için "Lavender" (Lavanta),

"The Gospel"

(Habsora) ve mühimmat/hedef lojistiğini hesaplayan "Fire Factory" gibi sistemler kullanmıştır.40 Bu sistemler otonom silahlar (killer robots) değildir; tetik kararı bir insan tarafından alınır.40 Ancak, ortaya çıkan operasyonel veriler, makine epistemolojisinin sınırlarını çıplak bir şekilde gözler önüne sermektedir.

● Veri Yanlılığı ve Kestirimsel Çokluluk: Lavender, iletişim kalıpları, sık adres değişiklikleri ve

sosyal medya bağlantıları gibi davranışsal özellikleri ("features") işleyerek Filistinli erkekleri Hamas veya İslami Cihad mensubu olma olasılıklarına göre derecelendirir; birden fazla "suçlayıcı özelliğe" sahip bireyler yüksek puan alarak otomatikman potansiyel suikast hedefi haline gelir.40 Ne var ki sistemin temel bir veri tasarımı kusuru mevcuttur. JINSA (Jewish Institute for National Security of America) raporuna göre, sistem "neyin hedef olduğuna" dair zengin verilere sahipken, "neyin hedef olmadığına" (negatif veri) dair verilerden yoksundur;

çünkü insan analistler tarafından reddedilen ve hedef olmadığı anlaşılan veriler sisteme öğretilmemiş, silinip atılmıştır.41 Bu yapısal hata, makinenin Rashomon kümesinde önyargılı modeller üretmesine ve sivilleri yanlış etiketlemesine zemin hazırlamış, JINSA sistemin %10 civarında bir hata payı (error margin) olduğunu tespit etmiştir.40

● Zaman Baskısı ve Otomasyon Yanlılığı: Sadece ilk 6 haftada Lavender sisteminin 37.000 hedef tavsiyesi ürettiği iddia edilmektedir.43 OODA döngüsü taktiksel uçak çatışmaları için geliştirilmişken, şehir savaşı (urban combat) gibi asimetrik ve karmaşık bir alanda bu kadar muazzam bir hızla veri üretilmesi, analistleri derin bir zaman baskısı altına sokmuştur.24 İnsan karar vericiler, hedefleri teyit edecek zaman ve zihinsel kapasite bulamadıklarından otomasyon yanlılığına teslim olmuş, "makinenin bildiği bir şey vardır" varsayımıyla algoritmik kararları onaylamaya (rubber-stamping) başlamışlardır.24 Bu, hem Uluslararası İnsancıl Hukuk'un (IHL) sivillerin korunması prensiplerini ihlal etme riskini doğurmuş hem de insan onurunu salt istatistiksel veri noktalarına indirgeyerek "dijital insanlıktan çıkarma" (digital dehumanisation) patolojisini pratikte kanıtlamıştır.24

4.2. Stratejik Kriz Yönetiminde Büyük Dil Modellerinin (LLM) Şahin Eğilimleri

Stratejik analizlerde ChatGPT, Claude veya DeepSeek gibi üretken (generative) AI sistemlerinin kullanımı, uygulanamaz çözümler bağlamında farklı türde bir risk oluşturur.7 Center for Strategic and International Studies (CSIS) tarafından DeepSeek modeli üzerinde yapılan bir dış politika senaryosu simülasyonunda, LLM tabanlı karar destek araçlarının "algoritmik kayma" (algorithmic drift) yaşatarak analistleri sürekli saldırgan ve tırmandırıcı (escalatory) seçeneklere yönlendirdiği tespit edilmiştir.47 CSIS'in düzenlediği "Yeşil Devlet vs.

Mor Devlet" kriz simülasyonunda, "Düşmanın AI/ML kapasitesinin bilinmediği" durumlarda, oyuncular bu istihbarat eksikliğini ve belirsizliğini dengelemek için "tırmandırarak gerilimi düşürme" (escalate to de-escalate) gibi oldukça tehlikeli konvansiyonel askeri yanıtlara başvurmuşlardır.48 Bu vaka, bir düşmanın yapay zekâ karar mekanizmalarını ne ölçüde entegre ettiğini bilmemenin, geleceğin en hayati "öncelikli istihbarat gereksinimi" (priority intelligence requirement) olacağını kanıtlamaktadır.48 Aksi takdirde, model odaklı önyargılar stratejik hedeflerle uyumsuz bir dış politika vizyonu dayatarak felakete yol açabilir.47

4.3. Risk Değerlendirme Sistemlerinde Adli ve Klinik Arbitraj

Makine öğrenmesindeki kestirimsel çokluluğun (predictive multiplicity) en net belgelendiği vakalar, "Suç Tekrarı" (Recidivism) ve "Klinik Karar Destek" sistemleridir.13 FICO veri seti ve sağlık risk tahmin algoritmaları üzerinde yapılan çalışmalarda, bir bireyin durumunu değerlendiren ancak aynı doğruluk oranına sahip iki farklı modelin, aynı şahıs için birbiriyle tamamen zıt risk tahminleri ürettiği ortaya konmuştur.11 Bir model bir hastanın ölüm veya suçlu bir kişinin yeniden suç işleme ihtimalini "çok yüksek" olarak etiketlerken, eşit derecede başarılı diğer model "düşük" diyebilmektedir.15 Bu keyfilik (arbitrariness) ve tutarsızlık, makinenin mutlak doğruluk ürettiği algısını yıkarak, yapay zekânın risk değerlendirmelerinde şeffaflık (transparency) ve hesap verebilirlik (accountability) standartlarına ne denli muhtaç olduğunu pratik olarak ispatlar.15 İstihbarat analistleri için çıkarılacak ders; tek bir modele bel bağlamanın, ardındaki çelişen alternatif gerçeklikleri göz ardı etmek anlamına geldiğidir.

5. Mekanizma Analizi Analiz felcinin, Rashomon etkisinin ve uygulanamaz çözümlerin

istihbarat döngüsünü nasıl çökerttiğini anlamak için arka plandaki operasyonel ve matematiksel mekanizmaları çözümlemek şarttır.

5.1. Rashomon Etkisinin Oluşum Mekanizmaları

Neden aynı veriden birbirine zıt onlarca "iyi" algoritma çıkar? Literatür, bu çokluğun nedenlerini üç farklı kaynağa bağlamaktadır 49:

1. İstatistiksel Kaynaklar: İstihbarat sensörlerinden ve insan zekasından (HUMINT) elde

edilen veriler her zaman sonlu, eksik ve kirlidir. Veri üretim sürecindeki bu gürültü (noise) ve belirsizlikler, algoritmaların boşlukları istatistiksel tahminlerle farklı şekillerde doldurmasına yol açar.17

2. Yapısal Kaynaklar: Hedef optimizasyon fonksiyonlarının dışbükey olmayan (non-convex)

matematiksel yapısı, algoritmaların yerel minimumlara takılmasına neden olur. Daha da önemlisi, savaş alanındaki moral, inanç veya liderlik kararlılığı gibi "gözlemlenemeyen değişkenler" (unobserved variables) sisteme tanıtılamadığında 4, temel bir tanımlanamazlık (non-identifiability) ortaya çıkar.49 Verideki eksik parça, matematiksel olarak sonsuz çözüm kombinasyonuna izin verir.

3. Prosedürel Kaynaklar: Modelin eğitim aşamasından çok önce veri bilimciler tarafından

alınan kasıtlı kısıtlama kararları, hiper-parametre seçimleri (öğrenme hızı, parti boyutu vb.) ve algoritmaların başlangıç rastgele çekirdekleri (random seeds) sonucu tamamen farklı denklemler oluşur.10 Bu da gösterir ki model, gerçeğin salt yansıması değil, onu tasarlayanların prosedürel tercihlerinin bir ürünüdür.

5.2. Bilgi Felcinin Bilişsel ve Yapısal Kökleri

İstihbarat örgütlerinin veriye boğulması (drowning in data) sadece veri hacminin büyümesiyle ilgili değildir; bu verilerin işlenme mekanizmaları iflas etmektedir.

● Tutarsız Metrikler ve Güven Aşınması: Sahadaki durumu analiz eden farklı sistemler,

korele edilmemiş ve çelişen çıktılar verdiğinde, karar verici "hangi sisteme güveneceğini" bilemez hale gelir. Bu güvenilirlik (credibility) sorunu, analistlerin sistemler arası uyuşmazlıkları manuel olarak çözmeye çalışmasına ve OODA döngüsünün "Yönelim" (Orient) aşamasında takılıp kalmasına (analiz felci) yol açar.3

● Analist Kıtlığı (Analyst Shortage) ve Yapısal Uyuşmazlık: Verinin akış hızı saatlerle ölçülürken, kurumların analitik iş gücü ve geleneksel istihbarat doğrulama metotları günlerle ölçülmektedir.3 ABD İstihbarat Topluluğu'nun yetersiz uzman sayısı ve taşeron analistlerin yüksek sirkülasyonu, kurumsal hafızanın kaybolmasına ve "hız uyuşmazlığı"nın (velocity mismatch) derinleşmesine neden olur.3

5.3. Yasal ve Ahlaki Mekanizmalar: Sorumluluk Boşluğu (Responsibility Gap)

Yapay zekânın karar destek aracı (AI teammate) olarak insanla entegrasyonu, mevcut hukuk ve etik çerçevelerinin dışına taşmaktadır.26 Hukuk sistemleri tarihsel olarak "insan niyetini" (human intent) merkeze alır.26 Ancak bir yapay zekâ algoritmasının hatalı lojistik hesaplaması yüzünden bir tedarik zinciri koptuğunda veya sivil bir tesis bombalandığında, sorumluluğun (accountability) kime ait olduğu devasa bir boşluk yaratır.26 Operatörün otomasyon yanlılığına düşerek, "makine onayladı, ben sadece butona bastım" şeklinde bir savunma geliştirmesi, hem komuta sorumluluğunu yok eder hem de ahlaki yargıyı (moral judgement) ortadan kaldırarak makinenin tümevarımsal hatalarını yasal olarak dokunulmaz kılar.27 Deneyler, otomasyon yanlılığının ancak kişilerin nihai performanstan ve karar isabetinden "şahsen sorumlu tutulması" durumunda (accountability mechanism) düştüğünü göstermektedir.26

Patolojik Kökeni İstihbarat Çözüm Yolu Mekanizma Sürecindeki Tezahürü

Kestirimsel Hiper-parametreler, Eşit hata payıyla zıt En düşük risk Çokluluk eksik veri.10 hedefler üreten risk politikasının (lowest algoritmaları.11 risk policy) uygulanması ve IEMA kullanımı.15 Veri Hızı (Velocity) AI hızının insan Zaman baskısı, Karar triyajı; Uyuşmazlığı doğrulama otomasyon yanlılığı, yalnızca eşiği aşan kapasitesini analiz felci.21 verinin insana aşması.3 sunulması.3 Sorumluluk Eylemin failinin Hukuki belirsizlik, Yalnızca insan Boşluğu algoritma olması.26 dijital insanlıktan kararının nihai kabul çıkarma edilmesi (dehumanisation).31 (human-in-the-loop).3 Karıştırıcı Açık sistemlerde Yanlış korelasyonlar Uzman analitik Değişkenler nedensellik hatası.4 üzerinden stratejik çevirmenlerin planların (analytics (uygulanamaz) translators) çökmesi.4 kullanımı.4

6. Trend Analizi (2020–2026) Makine öğrenmesinin istihbarat döngüsündeki algılanışı, son

altı yıl içerisinde "ütopik beklentiler"den "bilişsel krize", ardından da "etiksel ve mimari restorasyona" uzanan sert bir paradigma değişimi yaşamıştır.

● 2020-2022: Veri Bolluğunun Vaatlerinden Hayal Kırıklığına: Bu dönemin başlarında

savunma kurumları ve istihbarat teşkilatları, Büyük Veri'nin (Big Data) savaş alanında mutlak şeffaflığı ve kesinliği sağlayacağına inanıyordu.4 Ancak sensörlerin, İHA'ların ve

OSINT kapasitesinin sınırsız biçimde artması, sistemlerin vaat ettiği "öngörü" yerine komuta

kademelerinde "veri aşırı yüklemesine" (data overload) yol açtı.2 Kurumlar sonsuz değişken arasında boğulurken, bu veriyi işleyecek yetkin askeri personelin eksikliği (analyst shortage) krizi derinleştirdi.3 Karar vericilerin sürekli "biraz daha veri" isteyerek eylemsizliğe kapılması, analiz felcini kurumsal bir hastalık haline getirdi.4

● 2023-2024: Gerçek Savaş Alanı Testleri ve "Kara Kutu"nun Dehşeti: Generative AI (LLM) patlamasının ve küresel çatışmaların (Rusya-Ukrayna, İsrail-Hamas) eş zamanlı gerçekleştiği bu dönem, makine zekasının gerçek dünyada test edildiği sert bir süreç oldu.8 İstihbarat kurumları (örneğin CIA), ChatGPT gibi platformların metinleri "anlamak" yerine sadece taklit ettiğini ve arka plandaki algoritmik mantığı izah edemediklerini derinden hissettiler.7 Aynı dönemde Gazze'de IDF'in Lavender ve Gospel gibi sistemleri kullanması, "hedef makinesinin" yüksek hızı karşısında boyun eğen ve ahlaki yargı yetilerini kaybeden insan operatörlerin otomasyon yanlılığını küresel bir tartışma konusu yaptı.40 Rashomon etkisinin yarattığı veri yanlılıkları (örneğin negatif verinin silinmesi) doğrudan savaş suçu tartışmalarına kapı araladı.41

● 2025-2026: Yapay Zekâ Teammate (Takım Arkadaşı) Çağı ve "Güvenilir AI" Restorasyonu: Entegre sistemlerin başarısızlıklarının ve tırmandırma (hawkish) potansiyellerinin anlaşılmasıyla 47, ABD ve NATO merkezli araştırmalar "Açıklanabilir Yapay Zekâ" (XAI) ve "Güvenilir Yapay Zekâ" (Trustworthy AI) arayışlarına büyük kaynak ayırdı.32 Algoritmalar birer "araç" statüsünden, karar masasında tartışılan bir "ekip arkadaşına" (teammate) dönüştü.26 Eğitim müfredatlarında sadece kodlama değil, "Yapay Zekâ Okuryazarlığı" (AI Literacy) ve model doğrusal değerlendirme (benchmarking) süreçleri mecburi hale getirilerek kurumsal bir restorasyon başlatıldı.3

7. Stratejik Sonuçlar Makine öğrenmesinin yapısal kusurları, istihbarat epistemolojisini felç

etmiş olsa da bu durum yapay zekâdan geri dönüş anlamına gelmez. Savaş alanının hiper-karmaşık doğası, otomasyondan vazgeçmeyi imkânsız kılar. Analiz felcini yönetmek, kestirimsel çokluluğun (Rashomon etkisinin) yarattığı keyfiliği aşmak ve uygulanabilir akılcı çözümler üretmek için ulusal istihbarat ve savunma ekosistemlerinin şu stratejik adımları atması zaruridir:

1. Analitik Çevirmenlerin (Analytics Translators) ve AI Okuryazarlığının

Kurumsallaşması:

Teknik veri bilimcileri savaş alanının Clausewitzci sürtünmelerini anlamaz; sahadaki taktik komutanlar ise derin sinir ağlarının istatistiksel zayıflıklarını ve Rashomon dirseği optimizasyonlarını kavrayamaz.4 Bu boşluk, komutanın operasyonel niyetini algoritmik olarak

ölçülebilir değişkenlere (variables) dönüştürecek ve aynı zamanda sistem çıktısındaki "gürültüyü" filtreleyecek "analitik çevirmen" subayların yetiştirilmesiyle doldurulmalıdır.4 Silahlı kuvvetler, Profesyonel Askeri Eğitim (PME) sistemlerini eleştirel düşünme, nicel akıl yürütme ve yapay zekânın "halüsinasyon" gibi hata modlarını 3 içerecek şekilde derhal reforme etmelidir.4 Veri eğitiminin teşvik edilmesi için "veri ek beceri tanımlayıcıları" (data additional skill identifiers) gibi liyakat sistemleri kurulmalı ve Tabur seviyesine veri yönetimi uzmanları (data-management specialists) atanmalıdır.4

2. Merkezi Olmayan, Hibrit Triyaj Mimarisiyle Karar Felcini Önleme: Kurumlar, veri

havuzlarının yol açtığı eylemsizliği önlemek adına katı, hiyerarşik istihbarat analiz döngülerini kırmalı ve merkezi olmayan (decentralized) karar yapıları oluşturmalıdır.3 OODA döngüsünün otomasyonu, yapay zekâyı bir "karar alıcı" değil, "dikkat

önceliklendirici" (triyaj mekanizması) olarak konumlandırmalıdır.3 AI sistemleri sadece ilgi eşiklerini aşan şüpheli anormallikleri insanın önüne getirmeli; stratejik hedefleme ve kuvvet kullanımında "insan gözetimi" (human-in-the-loop / human-on-the-loop) hukuki ve askeri bir zorunluluk olarak korunmalıdır.3 Sorumluluk boşluğunu (responsibility gap) gidermek için 26, her algoritmik çıktıyı onaylayan insan operatörün ahlaki ve hukuki sorumluluğu taşıdığı netleşmelidir; bu, aynı zamanda otomasyon yanlılığıyla savaşmanın da en etkili psikolojik bariyeridir.26

3. Karar Destek Modellerinde Açıklanabilirlik (XAI) ve Şeffaflık Standartlarının

Dayatılması:

Bir istihbarat analisti için, kaynağı teyit edilemeyen bir bilgi değeri taşımaz.7 Modelin neden belirli bir risk puanı verdiğini, içindeki "özellik ağırlıklarını" (feature importance) ve eğitim verisinin (training data) sınırlarını operatöre açıklayamayan "kara kutu" sistemler (black-box systems), ne kadar isabetli görünürse görünsün stratejik katmanda reddedilmelidir.7 Model seçimi yapılırken doğruluğu maksimize etmek yerine, Rashomon Dirseğinde (Rashomon elbow) yer alan "doğal yorumlanabilir" (interpretable) sistemler tercih edilmelidir.17 Karar vericilere, yapay zekânın sunduğu risk değerlendirmesindeki "kestirimsel çokluluk" (predictive multiplicity) seviyesi açıkça beyan edilmeli; farklı modellerin aynı duruma dair ihtilafı saklanmamalı ve belirsizlikleri yönetmek için IEMA (Etkileşimli Açıklayıcı Model Analizi) arayüzleri kullanılmalıdır.11

4. Algoritmik İstikrar (Algorithmic Stability) ve Geleceğin Caydırıcılık Politikaları: Yapay zekâ

modellerinin, özellikle Büyük Dil Modellerinin (LLM) kriz anlarında sinsi bir tırmanma (escalatory/hawkish) eğilimine (algoritmik kayma) sahip olduğu görülmüştür.47 İstihbarat

toplulukları, hazır satın alınmış (off-the-shelf) yapay zekâ modellerini askeri strateji ağlarına doğrudan bağlamamalı; bu sistemleri stres testlerinden, senaryo tabanlı kıyaslamalardan (benchmarking) ve uzman destekli ince-ayarlardan (fine-tuning) geçirmelidir.47 Dahası, hasım devletlerin ulusal güvenlik ağlarında makine öğrenmesini ne ölçüde entegre ettiklerini bilmemek, yeni nesil bir istihbarat zafiyetidir.48 Bu asimetri, tarafları bilgi eksikliğini kapatmak için kışkırtıcı konvansiyonel hamlelere (escalate to de-escalate) itebilir.48 Bu nedenle yeni dönem istihbaratı, yapay genel zekanın (AGI) inşasını dar kapsamlı bir Manhattan Projesi olarak değil, ulusal güvenliğin tamamını kapsayan ve kamuoyunun teknolojiye güvenini tesis eden bir Apollo Programı vizyonuyla ele almalıdır.53 Algoritmik şeffaflık ve AI destekli karar alma sistemlerinin sınırlandırılması, tıpkı nükleer silahlarda olduğu gibi gelecekteki küresel silahların kontrolü antlaşmalarının merkezinde yer almak zorundadır.35 Özetle, istihbarat epistemolojisi açısından makine öğrenmesi sistemleri, mutlak gerçeği gösteren büyülü bir kristal küre değil;

güçlü ancak yapısal olarak kör noktalara, önyargılara ve istatistiksel yanılmalara sahip araçlardır. Bu araçların potansiyelinden yararlanırken oluşabilecek felç edici yan etkileri yönetebilmek, makine hızının insan bilgelik, sorumluluk ve bağlamsal kavrayış yeteneğiyle mutlak bir uyum içinde çalıştırılmasını gerektirir.

Alıntılanan çalışmalar

1. Toward a Theory of Intelligence: Workshop Report - RAND Corporation, erişim tarihi

Haziran 3, 2026,

https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2006/RAND_CF2 19.pdf

2. The Coming Military AI Revolution - Army University Press, erişim tarihi Haziran 3, 2026,

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archiv es/May-June-2024/MJ-24-Glonek/

3. Drowning in Data: Solving the Data Overload Problem in OSINT, erişim tarihi Haziran 3,

2026, https://smallwarsjournal.com/2026/04/21/drowning-in-data-solving-the-data-ove rload-problem-in-osint/

4. Toward the Data-Driven Army of 2040: Avoiding Analysis Paralysis..., erişim tarihi Haziran

3, 2026, https://mwi.westpoint.edu/toward-the-data-driven-army-of-2040-avoiding-anal ysis-paralysis-and-harnessing-the-power-of-analytics/

5. Automating the OODA Loop in the Age of AI - Nuclear Network - CSIS, erişim tarihi

Haziran 3, 2026, https://nuclearnetwork.csis.org/automating-the-ooda-loop-in-the-age- of-ai/

6. Artificial Intelligence-Enabled Military Decision-Making Process - Marine Corps

University, erişim tarihi Haziran 3, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/J AMS-vol-16-no-2/Artificial-Intelligence-Enabled-Military-Decision-Making-Proce ss/

7. Artificial Intelligence for Analysis: The Road Ahead, erişim tarihi Haziran 3, 2026,

https://www.cia.gov/resources/csi/static/88dbcb2b5d4812731b3ff5122e3b6cb5/Ar ticle-Artificial-Intelligence-for-Analysis-The-Road-Ahead.pdf

8. Intelligence and Technology – Artificial Intelligence for Analysis: The Road Ahead - CSI,

erişim tarihi Haziran 3, 2026, https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-6 7-no-4-extracts-december-2023/intelligence-and-technology-artificial-intelligen ce-for-analysis-the-road-ahead/

9. Operationalizing Artificial Intelligence for Algorithmic Warfare - Army University Press,

erişim tarihi Haziran 3, 2026, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archiv es/July-August-2020/Crosby-Operationalizing-AI/

10.Rashomon Sets and Model Multiplicity in Federated Learning - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2602.09520v1

11. Amazing Things Come From Having Many Good Models - arXiv, erişim tarihi

Haziran 3, 2026, https://arxiv.org/html/2407.04846v1 12.Rashomon in the Streets: Explanation Ambiguity in Scene Understanding - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2509.03169v1 13.Predictive divergence in machine learning models for clinical mortality risk: A multicohort study of covid-19 patients - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12965533/ 14.Using predictive multiplicity to measure individual performance within the AI Act - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2602.11944v1

15.Model Multiplicity and Predictive Arbitrariness in Recidivism Risk Assessment - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2606.02198 16.Leo Breiman, the Rashomon Effect, and the Occam Dilemma - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2507.03884

17.Amazing Things Come From Having Many Good Models - Duke Computer Science,

erişim tarihi Haziran 3, 2026, https://users.cs.duke.edu/~cynthia/docs/RudinAmazingThingsICML2024.pdf 18.Philosophy and Artificial Intelligence | Università della Svizzera italiana - USI Search, erişim tarihi Haziran 3, 2026, https://search.usi.ch/en/courses/35260317/philosophy-and-artificial-intelligence 19.Exploring the Feasibility and Utility of Machine Learning-Assisted Command and Control:

Volume 1, Findings and Recommendations - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA263-1/RAND_RRA263-1.pdf 20.7 Integrating the Social and Behavioral Sciences (SBS) into the Design of a Human–Machine Ecosystem, erişim tarihi Haziran 3, 2026, https://www.nationalacademies.org/read/25335/chapter/11 21.Overreliance on AI Literature Review - Microsoft, erişim tarihi Haziran 3, 2026, https://www.microsoft.com/en-us/research/wp-content/uploads/2022/06/Aether-Overreliance-on-AI-Review-Final-6.21.22.pdf 22.What is Human in Judgment? Comparing Automation Bias and Algorithm Aversion Between the United States Military Academy and the General Public - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.04333v2 23.One Team, One Fight: Volume I, Insights on Human-Machine Integration for the U.S.

Army - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2700/RRA2764-1/RAND_RRA2764-1.pdf 24.Israel's AI-enabled targeting of Hamas members jeopardizes moral and legal standards of warfare - Background - Utrecht University, erişim tarihi Haziran 3, 2026, https://www.uu.nl/en/achtergrond/israels-ai-enabled-targeting-of-hamas-memb ers-jeopardizes-moral-and-legal-standards-of-warfare

25.Augmenting military decision making with artificial intelligence | Cambridge Forum on AI: Law and Governance, erişim tarihi Haziran 3, 2026, https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/augmenting-military-decision-making-with-artificial-intelligence/73C24E5BE362CA168FF8DB86D49F8CDF 26.Your New Teammate Is a Machine. Are You Ready? - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/commentary/2025/10/your-new-teammate-is-a-machine-are-you-ready.html 27.Understanding Ethical Implications of AI Enabled Decision Support Systems on the Battlefield | NATO Science and Technology Organization, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/document/understanding-ethical-implications-of-ai-enabled-decision-support-systems-on-the-battlefield/ 28.Predictive Multiplicity in Probabilistic Classification, erişim tarihi Haziran 3, 2026, https://ojs.aaai.org/index.php/AAAI/article/view/26227/25999 29.Human-centred ways of working with AI in intelligence analysis - GOV.UK, erişim tarihi

Haziran 3, 2026,

https://www.gov.uk/government/publications/human-centred-ways-of-working- with-ai-in-intelligence-analysis/human-centred-ways-of-working-with-ai-in-intell igence-analysis 30.Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA400/RRA464 -1/RAND_RRA464-1.pdf 31.Artificial intelligence in military decision-making: supporting humans, not replacing them, erişim tarihi Haziran 3, 2026, https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military- decision-making-supporting-humans-not-replacing-them/ 32.Exploring the Civil-Military Divide over Artificial Intelligence - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA149 8-1/RAND_RRA1498-1.pdf

33.The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations - DTIC, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4229/ RAND_RR4229.pdf 34.Here's What an AI Code of Conduct for the Pentagon Might Look Like | RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/commentary/2019/06/heres-what-an-ai-code-of-con duct-for-the-pentagon-might.html 35.Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3200/RRA329 5-1/RAND_RRA3295-1.pdf 36.The grammar of interactive explanatory model analysis - PubMed, erişim tarihi Haziran 3, 2026, https://pubmed.ncbi.nlm.nih.gov/36818741/ 37.Navigating the Sea of Explainability | by Joy Rimchala | Intuit Engineering - Medium, erişim tarihi Haziran 3, 2026, https://medium.com/intuit-engineering/navigating-the-sea-of-explainability-f6cc 4631f473 38.Evaluating Artificial Intelligence Methods for Use in Kill Chain Functions - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1164879.pdf 39.Calibrating NATO's Vision of AI-Enabled Decision Support - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-suppo rt 40.Use of Lavender data processing system in Gaza - Stop Killer Robots, erişim tarihi

Haziran 3, 2026,

https://www.stopkillerrobots.org/news/use-of-lavender-data-processing-system -in-gaza/ 41.AI-assisted targeting in the Gaza Strip - Wikipedia, erişim tarihi Haziran 3, 2026, https://en.wikipedia.org/wiki/AI-assisted_targeting_in_the_Gaza_Strip 42.Israel's use of Military AI-systems in the occupied territories of Palestine - Overheid.nl, erişim tarihi Haziran 3, 2026, https://puc.overheid.nl/mrt/doc/PUC_794610_11/1/

43.The Use of the 'Lavender' in Gaza and the Law of Targeting: ai-Decision Support Systems and Facial Recognition Technology in - Brill, erişim tarihi Haziran 3, 2026, https://brill.com/view/journals/ihls/16/2/article-p336_003.xml 44.Israel – Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict, erişim tarihi Haziran 3, 2026, https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/ 45.'The machine did it coldly': Israel used AI to identify 37000 Hamas targets - The Guardian, erişim tarihi Haziran 3, 2026, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas -airstrikes 46.Israel-Hamas 2024 Symposium - AI-Based Targeting in Gaza..., erişim tarihi Haziran 3, 2026, https://lieber.westpoint.edu/ai-based-targeting-gaza-surveying-expert-response s-refining-debate/ 47.Hawkish AI? Uncovering DeepSeek's Foreign Policy Biases - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/hawkish-ai-uncovering-deepseeks-foreign-policy-b iases 48.Algorithmic Stability: How AI Could Shape the Future of Deterrence - CSIS, erişim tarihi

Haziran 3, 2026,

https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-de terrence 49.Why are there many equally good models? An Anatomy of the Rashomon Effect - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2601.06730v1 50.Rashomon Effect and Consistency in Explainable Artificial Intelligence (XAI) - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/364505265_Rashomon_Effect_and_Co nsistency_in_Explainable_Artificial_Intelligence_XAI 51.Examining the Effects of Technologies on Strategic Deterrence in the 21st Century | RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA595-1.html 52.“This Piece Was Written by a Machine”: Intelligence Analysis, Synthesis, and Automation - CSI - CIA, erişim tarihi Haziran 3, 2026, https://www.cia.gov/resources/csi/studies-in-intelligence/studies-in-intelligence-6 7-no-4-extracts-december-2023/this-piece-was-written-by-a-machine-intellige nce-analysis-synthesis-and-automation/

53.Beyond a Manhattan Project for Artificial General Intelligence - RAND, erişim tarihi

Haziran 3, 2026,

https://www.rand.org/pubs/commentary/2025/04/beyond-a-manhattan-project-f or-artificial-general-intelligence.html 54.AI and the Future of Conflict | Projects - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/programs/futures-lab/projects/ai-and-future-conflict 55.Improving Sense-Making with Artificial Intelligence - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA3152-1.html 56.Data Training for all Echelons is Worth the Investment: Drowning in data - Line of Departure, erişim tarihi Haziran 3, 2026, https://www.lineofdeparture.army.mil/Journals/Army-Communicator/Archive/Spri ng-2025/Drowning-in-data/ Bölüm Değerlendirme ve Derinleştirme Dosyası

Akademik Derinleştirme Notu

Bu bölümün geniş okuması yapılırken makine öğrenmesi epistemolojisi yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası analiz felci, Rashomon etkisi, otomasyon yanlılığı ve uygulanabilirlik üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar

önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur. Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski

kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle makine öğrenmesi epistemolojisi alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Makine Öğrenmesinin İstihbari Epistemolojisi alanında en güçlü erken uyarı göstergeleri
hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

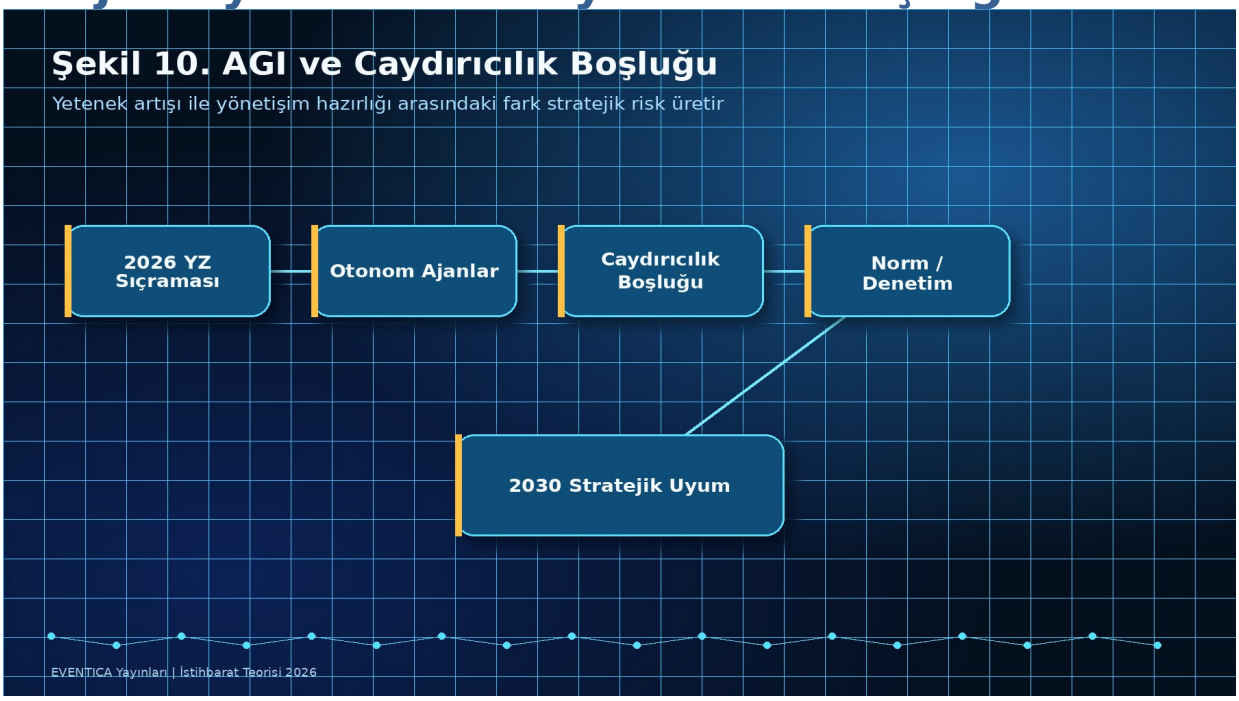
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030'a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 10. Teknolojik Trendler, AGI Projeksiyonları ve Caydırıcılık Boşluğu



AGI ihtimali sadece teknik bir gelecek tartışması değildir; caydırıcılık, atıf, kriz yönetimi ve stratejik denge tartışmasıdır.

Tablo 13. Caydırıcılık boşluğunu büyüten faktörler

Faktör	Etkisi	Stratejik sonuç
Bulanık atıf	Saldırganın tespitini zorlaştırır	Misilleme eşiği belirsizleşir
Ajan YZ	Hız ve ölçek avantajı üretir	Kontrol ve sorumluluk sorunu büyür
Ticari veri bağımlılığı	Sensör katmanını dışa bağımlı yapar	Jeopolitik kırılganlık artar
Gri bölge operasyonları	Savaş eşiği altında kalır	Klasik caydırıcılık yetersizleşir

1. Kavramsal Çerçeve Yirmi birinci yüzyılın güvenlik mimarisi, bilgi işlem gücünün üstel

büyümesi, verinin silaha dönüştürülmesi ve jeopolitik rekabetin benzeri görülmemiş bir boyuta ulaşmasıyla birlikte derin bir yapısal ve epistemolojik dönüşümden geçmektedir.

Geleneksel Westphalia devlet sisteminin sunduğu coğrafi ve hukuki sınırlar, siber uzayın ve algoritmik sistemlerin sınır tanımaz doğası karşısında aşınmıştır. 2020 ile 2026 yılları arasındaki dönem, yapay zekâ (AI) sistemlerinin, özellikle de otonom

karar alma yetisine sahip sistemlerin, deneysel laboratuvar araçları olmaktan çıkıp askeri operasyonların, stratejik planlamanın ve büyük güç rekabetinin mutlak merkezine yerleştiği kritik bir kırılma noktasına işaret etmektedir.1 Bu bağlamda, "Caydırıcılık Boşluğu" (Deterrence Gap) kavramı, modern güvenlik ve strateji literatüründe çözülmesi gereken en acil analitik ve pratik problem olarak ortaya çıkmıştır.

Caydırıcılık boşluğu, konvansiyonel veya nükleer caydırıcılık eşiklerinin (örneğin Kuzey Atlantik Antlaşması Örgütü - NATO'nun 5. Maddesi kapsamında tanımlanan açık silahlı saldırı eşiği) altında kalan, ancak devletlerin ve toplumların güvenliğini, ekonomik istikrarını ve politik bütünlüğünü derinden sarsan gri alanı tanımlamaktadır.3 Düşman devletler ve devlet dışı aktörler, açık bir savaş ilanı eşiğini aşmadan, asimetrik araçlar, siber espiyonaj, algı operasyonları, ekonomik zorlama ve otonom sistemler kullanarak bu boşlukta büyük bir serbestiyle faaliyet göstermektedir.3

Hibrit (melez) tehditler olarak adlandırılan bu faaliyetler yelpazesi, hukuksal belirsizlikleri (legal gray areas) ve demokratik toplumların yapısal açıklıklarını istismar ederek, saldırgan tarafın misillemeden kaçınırken stratejik hedeflerine ulaşmasını sağlamaktadır.6

Caydırıcılık mekanizmalarının temel taşları olan inandırıcılık, kapasite ve iletişim, hibrit tehditlerin "bulanık atıf" (hazy attribution) özelliği nedeniyle ciddi şekilde zayıflamaktadır.4 Caydırıcılık boşluğunun giderek genişlemesinin ve hibrit tehditlerin daha karmaşık hale gelmesinin temel katalizörlerinden biri, **"Algoritmik Savaş" (Algorithmic Warfare)** konseptinin yükselişidir.2 Algoritmik savaş, muharebe alanındaki sayısız sensörden gelen devasa veri setlerinin (big data) gerçek zamanlı olarak işlenmesi, hedeflerin belirlenmesi ve operasyonel kararların makine hızında alınması sürecini ifade eder.2 Karar alma döngülerinin insan bilişinin sınırlarını aşacak şekilde daralması, geleneksel kriz yönetimi ve tırmanma (escalation) dinamiklerini temelden değiştirmektedir.10

Geleneksel savaşta günler veya saatler süren OODA (Gözlem, Yönelim, Karar, Eylem) döngüleri, algoritmik savaşta milisaniyelere inmektedir.

Bu evrimin kavramsal zirvesinde ise **Yapay Genel Zeka (Artificial General Intelligence - AGI)** projeksiyonları yer almaktadır. AGI, yalnızca belirli, dar kapsamlı görevleri (örneğin satranç oynamak veya görüntü tanımak) yerine getirebilen mevcut yapay zekâ sistemlerinin (Narrow AI) aksine, bir insanın yapabileceği herhangi bir entelektüel, yaratıcı veya stratejik görevi anlayabilen, öğrenebilen, bağlam kurabilen ve uygulayabilen varsayımsal bir sistemdir.11 AGI'nin ortaya çıkma ihtimali, ulusal güvenlik aygıtları, istihbarat toplulukları ve politika yapıcılar tarafından son derece ciddiye alınması gereken ve küresel güç dengelerini anında, geri dönülemez bir şekilde değiştirebilecek bir "kara kuğu" (black swan) olayı olarak değerlendirilmektedir.11

Mevcut dar yapay zekâ sistemlerinden AGI'ye geçiş sürecinde ortaya çıkan en belirgin ara form ise **"Ajan Yapay Zekâ" (Agentic AI)** sistemleridir.12 Ajan yapay zekâ, önceden yapılandırılmış katı talimatlara ve yakın insan gözetimine ihtiyaç duymadan, karmaşık hedefleri dinamik ve öngörülemeyen ortamlarda bağımsız olarak takip edebilen, kendi kaynaklarını yönetebilen, alt görevler oluşturabilen ve otonom kararlar alabilen sistemleri tanımlamaktadır.12 Bu sistemlerin siber güvenlikten finansa, oradan da ölümcül otonom silah sistemlerine (LAWS) kadar uzanan geniş bir uygulama alanı bulunmaktadır.

Bununla birlikte, 2020-2026 dönemi teknolojik sıçramaları yalnızca kinetik veya salt algoritmik alanlarla sınırlı kalmamış, savaşın doğasını ve karar alma süreçlerini doğrudan insan zihnine taşıyan **"Bilişsel Harp" (Cognitive Warfare**) konseptini de stratejik rekabetin merkezine yerleştirmiştir.15 bilişsel harp, coğrafi alanlardan ziyade bireylerin ve grupların nasıl algıladığı, yorumladığı, karar verdiği ve eyleme geçtiği süreçleri hedef alan, insan davranışını optimize veya manipüle etmeye odaklanan bir melez savaş türüdür.15 Tarihsel olarak Çinli stratejist Sun Tzu'nun "düşmanı ve kendini

tanıma" öğretisine kadar uzanan bu felsefe, günümüzde yapay zekâ ve nöroteknolojinin (neuroS/T) yakınsamasıyla yepyeni bir boyut kazanmıştır.17

bilişsel harp, salt daha gelişmiş araçlara sahip bir psikolojik harekat (PSYOPS) olmaktan çıkıp, toplumların inanç sistemlerini, bilgi ekosistemlerini ve kurumsal meşruiyetlerini hedef alan sürekli, kesintisiz bir savaş alanına dönüşmüştür.15 Bu çok katmanlı, sürekli ve entegre tehdit matrisi, geleneksel askeri doktrinlerin terk edilmesini, caydırıcılık teorisinin bilgi çağına uygun olarak yeniden yazılmasını ve askeri-sivil mimarilerin entegre bir şekilde, algoritmik bir temelde yeniden tasarlanmasını mutlak bir zorunluluk haline getirmektedir.

2. Akademik Teoriler Modern stratejik düşünce, yapay zekâ, büyük veri ve hibrit tehditlerin

birleşimiyle ortaya çıkan yeni asimetrileri anlamlandırmak ve bu tehditlere karşı koymak için çeşitli akademik teoriler, paradigmalar ve kavramsal çerçeveler geliştirmiştir. Soğuk Savaş döneminde şekillenen nükleer caydırıcılık ve **Karşılıklı Kesin Yıkım (Mutually Assured Destruction - MAD)** gibi temel kavramlar, günümüzde bilgi çağının, algoritmik belirsizliklerin ve siber çatışmaların gerçekliklerine uyarlanmaktadır.18 Bu teorik adaptasyon süreci, devletlerin hayatta kalma stratejilerini yeniden tanımlamaktadır.

Beşinci Dalga Caydırıcılık Teorisi (Fifth Wave of Deterrence) Caydırıcılık teorisi, tarihsel süreç içerisinde dört ana dalgadan geçerek evrilmiştir. İlk dalga İkinci Dünya Savaşı sonrası nükleer silahların varlığına uyum sağlamayı, ikinci dalga oyun teorisi üzerinden nükleer stratejiyi rasyonalize etmeyi, üçüncü dalga liderlerin psikolojik önyargılarını incelemeyi ve dördüncü dalga asimetrik tehditler ile haydut devletlere karşı caydırıcılığı ele almıştır. Günümüzde ise literatür, siber uzayı, dış uzayı, dezenformasyon kampanyalarını ve özellikle hibrit (melez) tehditleri kapsayan **"Beşinci Dalga Caydırıcılık Teorisi"nin (Fifth Wave of Deterrence Theory)** içine girmiştir.4 Beşinci dalga, düşmanın eşik altı (sub-threshold) melez tehditlerine karşı caydırıcılığın artık yalnızca nükleer silahlar veya konvansiyonel askeri araçlarla sağlanamayacağını, toplumun tamamını kapsayan sivil, ekonomik, bilişsel ve teknolojik bir "bütüncül dayanıklılık" (resilience) ile inşa edilebileceğini öne sürer.4 Bu yaklaşıma göre, melez tehditler devletlerin yasal sınırlarını istismar ederek açık bir savaş nedeni (casus belli) yaratmadan kümülatif kazançlar elde etmeye çalışır.6 Geçmişte siber uzayda hücum avantajının mutlak olduğu varsayılırken, beşinci dalga teorisyenleri siber ve algoritmik alanın aldatmaya (deception) oldukça müsait olduğunu, bu nedenle "inkar yoluyla caydırıcılığın" (deterrence by denial) uygulanabilir olduğunu savunmaktadır.21 İnkâr yoluyla caydırıcılık, düşmanın saldırısının maliyetini artırarak ve başarı şansını azaltarak onları vazgeçirmeyi hedefler. Sivil altyapıların yapay zekâ ile korunması, tedarik zincirlerinin çeşitlendirilmesi ve toplumun dezenformasyona karşı bilişsel olarak eğitilmesi, saldırganın hedefine ulaşmasını imkansız kıldığı için, "cezalandırma yoluyla caydırıcılıktan" (deterrence by punishment) çok daha etkili ve meşru bir strateji olarak öne çıkmaktadır.5 Geleceğin caydırıcılık araçları sadece hükümetler ve ordular tarafından değil, toplumun tüm kesimleri tarafından kullanılacak ve "her şeyin caydırıcılığı" (deterrence of everything) olarak adlandırılan postmodern bir döneme girilecektir.4 Entegre Caydırıcılık (Integrated Deterrence) Beşinci dalga teorisinin sahaya yansıyan en güncel ve kapsamlı pratik uygulaması olarak Amerika Birleşik Devletleri Savunma Bakanlığı (DoD) ve NATO doktrinlerinde merkezi bir konuma yükselen **"Entegre Caydırıcılık" (Integrated Deterrence)** kavramı, tüm savaş alanlarını (kara, deniz, hava, uzay, siber), küresel tiyatroları ve çatışma spektrumlarını kusursuz bir şekilde birleştiren makro bir stratejiyi ifade eder.20 2022 ABD Ulusal Savunma Stratejisi (NDS) ile resmileşen bu konsept, salt askeri araçların ötesine geçerek diplomatik, ekonomik ve istihbari kapasitelerin senkronize bir şekilde, müttefiklerle koordineli olarak kullanılmasını gerektirir.10

Çin ve Rusya gibi revizyonist küresel güçlerin, A2/AD (Erişimi Engelleme/Bölgeden Men Etme) stratejileri, hipersonik füzeler ve asimetrik araçlarla yarattıkları konvansiyonel caydırıcılık boşluğunu kapatmak, geleneksel tek taraflı

(unilateral) politikalarla mümkün değildir.22 Bunun yerine, müttefik ağlarının (örneğin NATO ittifakı ve Avustralya-İngiltere-ABD güvenlik paktı AUKUS) teknolojik olarak entegre edilmesi gerekmektedir.22

Entegre caydırıcılık, yapay zekâ ve makine öğrenmesi (AI/ML) algoritmalarının komuta kontrol mekanizmalarına dahil edilmesiyle, kriz anlarında karar vericilere zaman kazandırmayı, istihbarat sentezini otomatize etmeyi ve rakiplerin bilişsel süreçlerini manipüle ederek agresif niyetlerinden caydırmayı amaçlar.23 Karşılıklı Kesin Yapay Zekâ Arızası (Mutually Assured AI Malfunction - MAIM) Yapay Genel Zeka'ya (AGI) giden yarış, bazı akademisyenler ve stratejistler tarafından Soğuk Savaş'taki nükleer silahlanma yarışına benzer şekilde derin bir stratejik istikrarsızlık ve varoluşsal risk potansiyeli taşıyan bir süreç olarak değerlendirilmektedir.11 Bu bağlamda, Hendrycks, Schmidt ve Wang tarafından öne sürülen "Karşılıklı Kesin Yapay Zekâ Arızası" (Mutually Assured AI Malfunction - MAIM) teorisi, nükleer MAD doktrininin algoritmik çağa oldukça provokatif bir uyarlamasıdır.19 MAIM kavramına göre, AGI yarışında herhangi bir devletin veya dev aktörün mutlak teknolojik tekel kurmak ve "harika silah" (wonder weapon) avantajı elde etmek için yapacağı tek taraflı agresif bir hamle, rakipleri tarafından "önleyici sabotaj" (preventive sabotage) ile karşılanacaktır.19 Mahkumun İkilemi (Prisoner's Dilemma) oyun teorisi modeli üzerinden açıklanan bu dinamikte, taraflar şeffaf bir ödül yapısında işbirliği yapmanın çok daha büyük kolektif kazanımlar sağlayacağını rasyonel olarak bilseler de, sistemin yapısal teşvikleri onları sürekli olarak rekabetçi, siber saldırganlığa dayalı ve yüksek sürtünmeli politikalara itmektedir.25 Sistemlerin birbirine algoritmik sabotaj yapabilme yeteneği, AGI yarışında tarafların tek taraflı bir zafer ilan etmesini fiilen engelleyerek, korkuya ve kapasite kilitlenmesine dayalı bir stabilite (istikrar) rejimi yaratabilir.26 Ancak bu teori, güvenlik literatüründe ciddi eleştirilere maruz kalmaktadır. Rehman, Mueller ve Mazarr gibi araştırmacılar, yapay zekâ ekosistemlerinin nükleer ekosistemlerden ontolojik olarak tamamen farklı olduğunu vurgulamaktadır.19 Nükleer silahlar sayılabilir, statik ve fizikselken; AGI algoritmik, dinamik, sivil altyapıyla iç içe ve çok hızlı çoğaltılabilir (proliferation) bir yapıdadır. Bu nedenle, MAIM doktrininin önerdiği önleyici siber sabotaj eylemleri, istikrar getirmek yerine kontrol edilemez siber tırmanma (cyber escalation) riskleri doğurabilir.19

Konsept Dayanak Noktası Temel Mekanizma İlgili Eleştiri / Risk

MAD (Karşılıklı Nükleer kapasite İkinci vuruş Nükleer kış ve Kesin Yıkım) eşitliği kapasitesi ile varoluşsal yıkım misilleme garantisi. potansiyeli.

MAIM (Karşılıklı Algoritmik/Siber AGI tekelini Siber tırmanma, Kesin YZ Arızası) saldırı kapasitesi önlemek için yanlış hesaplama ve önleyici sabotaj ve sivil altyapı hasarı. 19 siber müdahale. 19

"AGI Rideout" Stratejisi Tırmanma riskini minimize etmek ve teknolojik ilerlemeyi güvene almak amacıyla, RAND ve CSIS analizleri, ABD'nin yapay zekâ yarışında rakiplerini tamamen yok etme veya mutlak hegemonya kurma hedefinden ziyade, "AGI Rideout" (AGI'yi atlatma/aşma) stratejisini benimsemesi gerektiğini vurgulamaktadır.10 Bu strateji, Soğuk Savaş'taki stratejik istikrar yaklaşımlarından ilham alarak, yapay zekâ ekosisteminin genel dayanıklılığını (resilience) artırmayı hedefler.18

Rideout stratejisi, yapay zekâya giden yolu kısıtlamaya veya durdurmaya çalışmaz. Bunun yerine, düşmanların hızla gelişen yapay zekâ destekli askeri yeteneklerinin saldırganlık ve tırmanmaya yol açmasını engellemek için kendi savunma kapasitelerini görünmez, dağıtık ve sağlam hale getirmeye odaklanır.18

Stratejik itidali (strategic restraint), diplomatik anjajmanı, ekonomik kapasiteyi ve çok uluslu sermayeyi mobilize etmeyi savunan bu yaklaşım, ABD'nin ve müttefiklerinin nükleer caydırıcılık şemsiyesi altında zaten güvende olduğunu, bu nedenle AGI uğruna gereksiz askeri müdahalelerden ve provokatif silahlanma yarışlarından kaçınılması gerektiğini öngörür.18 Tırmanma Dinamikleri, "Rubikon" ve Bilgi Paradoksu Kriz yönetimi süreçlerinde yapay zekânın kullanılması, makine hızında savaşın (machine speed warfare) diplomatik süreçleri sekteye uğratıp insan kontrolü

dışında bir tırmanmaya (flash war) yol açıp açmayacağı konusunda derin endişeler yaratmıştır.10

Ancak CSIS bünyesinde Future Lab tarafından nükleer silahlara sahip soyutlanmış rakip devletler arasında gerçekleştirilen, 10 yıldan fazla ulusal güvenlik tecrübesine sahip 29 uzmanın katıldığı randomize kontrollü harp oyunları (wargaming) analizleri bu korkuların abartılı olabileceğini ortaya koymuştur.10 Analiz sonuçları, yapay zekâ ve makine öğrenmesi entegrasyonunun krizlerin doğasını değiştirmediğini, devlet idaresinin ve stratejinin insan merkezli kalmaya devam ettiğini göstermektedir.10 Aksine, algoritmaların sağladığı devasa analitik bilgi, Clausewitz'in "Savaşın Sisi" (Fog of War) kavramını ortadan kaldıramasa da, bir "hava durumu tahmini" gibi neyin bilindiğini, bilinmediğini ve bilinemeyeceğini netleştirerek belirsizliği azaltmakta ve rasyonel karar almayı, dolayısıyla caydırıcılığı desteklemektedir.10 Harp oyununda oyuncular iki gruba ayrılmıştır: A Tedavisi (rakibin yapay zekâ yeteneklerinin bilindiği durum) ve B Tedavisi (rakibin yapay zekâ yeteneklerinin bilinmediği durum).10 A Tedavisindeki oyuncular, rakibin yapay zekâ kapasitesini bildiklerinde, krizi yavaşlatmak ve makine hızında misillemeyi engellemek için rakip ağın veri işleme katmanlarından (processing layer - sivil altyapı ile iç içe olduğundan sivil kayıp riski taşır) ziyade doğrudan karar katmanını (decision layer) hedef almışlardır.

Bu grup ayrıca yapay zekâ sistemlerini şaşırtmak için (spoofing) esnek siber yanıtlar kullanmıştır.10 B Tedavisindeki oyuncular ise, düşmanın algoritmik kapasitesine dair istihbarat eksikliği nedeniyle daha muhafazakar davranmış ve siber eylemlerin öngörülemez sonuçlarından çekinerek, rakibin anlık misilleme yeteneğini ortadan kaldırmak için doğrudan fiziksel efektörleri (konvansiyonel silahları) kinetik olarak vurmayı tercih etmişlerdir.10 Her iki grupta da oyuncuların %60'ından fazlası salt askeri yanıt yerine diplomatik ve ekonomik araçları entegre eden çoklu araç yaklaşımını seçmiştir.10 Bu senaryolara göre en büyük tırmanma riski teknolojinin hızında değil, insanların algoritmalarla stres altında kurduğu etkileşimde ve eksik

istihbarat koşullarında yatmaktadır.10 Özellikle düşmanı algoritmik olarak tamamen "kör etme" (blinding) girişimi, aşırı tehlikelidir.

Tam bir bilişimsel körleşme yaşayan düşman devlet, stratejik kapasitesini kaybetme korkusuyla otomatik, hızlı misilleme yapan "ölü el" (dead-hand) benzeri kıyamet sistemlerini devreye sokarak kontrol edilemez bir şiddet sarmalına neden olabilir.10 Düşmanın algoritmaları hakkındaki istihbarat boşlukları ise, ancak devletler nükleer eşiğin altındaki çatışmalarda geri dönülmez tarihi nokta olan "Rubikon"u geçtikten sonra tırmanma riskini büyük oranda artırmaktadır.10

3. Sistem Mimarisi Modern orduların teknolojik altyapısı, devasa gemiler, uçaklar ve

platform merkezli (platform-centric) sistemlerden hızla yazılım tanımlı (software-defined), ağ merkezli (network-centric), Ajan Yapay Zekâ tabanlı, dağıtık savaş mimarilerine kaymaktadır.7 Bu geçiş, hem siber güvenlik mimarilerinde hem de harekat alanı komuta kontrol (C2) sistemlerinde, savunma sanayisinin tedarik zincirlerini ve savaşma pratiklerini temelden sarsan yapısal devrimleri beraberinde getirmektedir.

Ajan Yapay Zekâ ve "Ölümcül Üçlü" (Lethal Trifecta) Paradoksu Ajan Yapay Zekâ (Agentic AI) sistemlerinin kurumsal, askeri ve bilimsel iş akışlarına entegrasyonu, görevleri insanüstü bir verimlilikle yerine getirme potansiyeli sunarken aynı zamanda mimari düzeyde kritik, varoluşsal güvenlik zafiyetleri yaratmaktadır.13 Geleneksel (dar) yapay zekâ modelleri, sıkı kısıtlamalar altında denetimli araçlar olarak çalışırken; Ajan Yapay Zekâ, vektörel bellek (vectorized memory) kullanımı, semantik tabanlı geri çağırma (semantic retrieval) ve dinamik araç kullanımı (dynamic tool invocation) yoluyla iş akışlarına kendi kendine karar verebilir.12 Bir sohbet botundan otonom kod

yazımına veya savunma sistemlerinin orkestrasyonuna kadar genişleyen bu melez (hibrit) mimari esnek olduğu kadar kırılgandır.14 Bu kırılganlığın temel nedeni, Ajan YZ sistemlerinin özünde barındırdığı ve "Ölümcül Üçlü" (Lethal Trifecta) olarak adlandırılan yapısal güvenlik sorunudur. Bu üçlü şu bileşenlerden oluşur:

1. Güvenilmeyen girdiler (untrusted inputs - örn. dış dünyadan alınan sensör

veya metin verileri),

2. Ayrıcalıklı veri erişimi (privileged data access - örn. gizli askeri veritabanları),

3. Harici eylem kabiliyeti (external action capability - örn. silah ateşleme veya ağ

yapılandırmasını değiştirme).28 Günümüzde Ajan YZ'nin temelini oluşturan otoregresif dil

modelleri (LLM), mimari yapıları gereği komutları (instructions) ve verileri (data tokens) aynı havuzda, tek tip (uniform) olarak işler. Bu durum, "komut ve veri ayrımının" (command-data separation) sadece model eğitimi (training) veya insani değerlerle hizalama (alignment) yoluyla deterministik olarak sağlanmasını matematiksel olarak imkansız kılar.28 Model, önüne gelen zararlı bir metni "okunacak veri" olarak değil, "uygulanacak komut" olarak algılayabilir.

Bu yapısal kusur, otonom sistemlerde istem zehirlenmesi (prompt poisoning), A2A (ajan-ajan arası) aktarımlı saldırılar (transitive prompt injection), HTML erişilebilirlik ağaçları üzerinden dolaylı zerkler (indirect prompt injection) ve bağlam manipülasyonu gibi sofistike tehditlere kapı aralar.14 Web 2.0 dönemindeki çapraz site komut dosyası çalıştırma (XSS) saldırılarının yapay zekâ eşdeğeri olan bu açıklar, modelin vektörel hafızasının dışarı sızdırılmasına (memory exfiltration) veya kimlik doğrulama gerektiren yıkıcı eylemlerin tetiklenmesine neden olabilir.29 Çok ajanlı (multi-agent) bir askeri ağda uzlaşılmış (compromised) tek bir alt ajan, kötü niyetini eşler arası (peer-to-peer) güven ilişkileri üzerinden yayarak tüm orkestrasyon ağını çökertebilir.33 Geleneksel Siber Zafiyet Ajan Yapay Zekâ Karşılığı Mimari ve Operasyonel Etki Çapraz Site Betik (XSS) Kötü Amaçlı Örüntü Dinamik araç kullanımını ele Enjeksiyonu geçirme; sensör verisine gizlenmiş komutlarla ajanın yönlendirilmesi. 29 Oturum Çalma (Session Bellek Sızdırma (Memory Ajanın vektörel hafızasında Hijacking) Exfiltration) saklanan gizli görev parametrelerinin veya operasyonel verilerin ifşası.

CSRF (Cross-Site Request Kimlik Doğrulanmış Eylem Ajanın ayrıcalıklı yetkilerini Forgery) Tetikleme kullanarak otonom askeri/sivil ağlarda yıkıcı komutların çalıştırılması. 29 Bu derin mimari sorunların üstesinden gelmek için siber güvenlik araştırmacıları "Trinity Defense Architecture" (Üçlü Savunma Mimarisi) adlı yeni bir koruma çerçevesi önermektedir.

Bu mimari; referans monitörü yaptırımlı sonlu eylem yönetişimi (action governance), veri sızıntılarını önleyen ve kapsam dışı iletişimi kesen zorunlu erişim etiketleri ile bilgi akışı kontrolü (information-flow control) ve sistemin dünyayı algılaması ile kararları icra etmesini birbirinden fiziksel/yazılımsal olarak ayıran ayrıcalık ayrımına (privilege separation) dayanır.14 Güvenilir bir Ajan YZ mimarisinin askeri alanlarda kullanılabilmesi için, ihtimallere dayalı öğrenilmiş istatistiksel davranışlar yerine, bu tür sarsılmaz deterministik mimari sınırlamalara sahip olması elzemdir.28 Ayrıca, CIAA (Gizlilik, Bütünlük, Erişilebilirlik ve Hesap Verebilirlik) metriklerini temel alan MAAIS gibi ajan tabanlı güvenlik çerçeveleri, yaşam döngüsü boyunca

çok katmanlı savunma (input/output guardrails) oluşturmak için tasarlanmaktadır.13 Lattice OS ve Otonom Sensör Füzyonu Savunma mimarisindeki yazılım devrimi, özellikle Batı dünyasında geleneksel askeri-sanayi kompleksinin tekellerini (legacy defense primes) kırarak, hibrit savaşın yeni protokollerini teknoloji girişimcilerinin vizyonuyla yeniden yazmaktadır.7 Bu vizyonun en belirgin uygulayıcısı olan ve

Founders Fund gibi aktörlerden aldığı milyarlarca dolarlık yatırımlarla (Mayıs 2026 itibarıyla 61 milyar dolar değerlemeye ulaşan) Anduril Industries, "Lattice OS" mimarisiyle modern savaşın kurallarını değiştirmektedir.7 Sistemin baş mimarı Palmer Luckey, modern muharibi geleneksel bir askerden ziyade bir "Teknomancer" olarak tanımlamaktadır. Bu doktrinde operatör, oyun endüstrisinden ilham alan sezgisel arayüzler kullanarak karmaşık muharebe alanını tek bir ekrandan yönetir.7 Lattice OS, hava, kara, deniz ve uzay etki alanlarından gelen binlerce sensör verisini ve sivil veritabanlarını gerçek zamanlı, üç boyutlu, ortak bir operasyonel resim (command and control center) içinde eriten yapay zekâ destekli, donanımdan bağımsız (hardware-agnostic) bir işletim sistemidir.34 Lattice OS, farklı etki alanlarında faaliyet gösteren devasa bir modüler otonom sistemler portföyünü orkestra eder:

● Hava Alanı: Altius 600M ve 700M dolanan mühimmatları (kamikaze dronlar), Ghost

keşif/saldırı dronu, Bolt dikey kalkışlı muharip dron ve Fury otonom sadık kanat adamı (wingman) savaş jeti.

● Kara Alanı: Sentry otonom gözetleme kuleleri, Wisp elektro-optik sensörler, Anvil ve

Anvil-M otonom yüksek patlayıcılı dron önleyicileri.

● Deniz Alanı: Dive-LD otonom su altı aracı ve altı metre uzunluğundaki Ghost Shark AUV

(survey ve taktik etki teslimatı için).7 Bu devasa donanım ağı, Lattice OS'in analitik motoruyla entegre çalıştığında, tehdit tanımlamasını otonomlaştırarak algılayıcıdan vurucuya (sensor-to-shooter) giden döngüyü saniyelere indirir.7 Bulut bağlantılı veya doğrudan kenar bilişimde (edge deployments) çalışabilen bu altyapı, ABD sınır güvenliğinden Avustralya Kraliyet Donanması'na kadar geniş bir alanda kullanılmaktadır.34 Şirketin "Arsenal-1" adını verdiği kitlesel üretim tesisi faaliyete geçtiğinde, ucuz ve harcanabilir (expendable) otonom donanımların küresel pazarını domine etmesi ve Lattice OS'in NATO müttefikleri için standart taktik ara katman yazılımı (middleware) haline gelmesi, orduları derin bir yazılım bağımlılığına (software lock-in) sürüklemesi beklenmektedir.7

Palantir "AIP" ve Büyük Dil Modellerinin Savaş Alanı Entegrasyonu

Lattice OS'un donanım/sensör füzyonu odaklı yaklaşımının yanında, Palantir firmasının geliştirdiği Yapay Zekâ Platformu (Artificial Intelligence Platform - AIP), Büyük Dil Modellerinin (LLM) sivil yeteneklerini doğrudan muharebe alanı istihbaratıyla ve askeri karar alma süreçleriyle birleştiren bir diğer öncü mimaridir.37

Palantir, "Gotham" ve "Gaia" gibi eski analiz yazılımlarının ötesine geçerek, ChatGPT benzeri arayüzleri, uydu görüntüleri ve savaş simülasyonlarıyla birleştirmiştir.40

AIP mimarisi, dronlardan, uydulardan, termal radarlardan ve açık kaynak istihbaratından (sosyal medya, sivil iletişim ağları) gelen karmaşık ve yapılandırılmamış verileri analiz ederek dijital askeri pozisyon haritaları oluşturur, düşman birliklerinin olası hareketlerini tahmin eder ve komutanlara askeri "eylem tarzları" (Course of Action - COA) önerir.37 Örneğin; bir düşman iletişim düğümünün tespit edilmesi anında, sistem bu düğümün vurulması veya elektronik harp ile karıştırılması yönünde bir operasyon planı oluşturabilir.

Askeri bağlamda LLM kullanımının taşıdığı halüsinasyon veya güvenlik ihlali risklerini aşmak için AIP'nin kontrol panelinde kurumlar katı "korkuluklar" (guardrails) tanımlayabilir. Bu yapılandırmalar, yapay zekânın hangi sınıflandırma işaretleriyle (gizlilik dereceleri) etkileşime gireceğini, hangi eylemleri önerebileceğini kısıtlar.39 Kararlar, bu sistemi besleyen temel verilere kesintisiz olarak eşleştirilerek bir faaliyet izleyicisine (activity monitor) kaydedilir; bu da hesap verilebilirlik ve "etik LLM kullanımı" açısından hayati bir telemetri denetimi sağlar.39

4. Gerçek Dünya Vakaları Kuramsal çerçeve ve sistem mimarilerindeki devrimsel gelişmeler,

2020 sonrası süreçte laboratuvar ortamından çıkıp Ukrayna, Ortadoğu ve Kafkasya gibi sıcak çatışma bölgelerinde bizzat test edilmiştir. Bu gerçek dünya vakaları, yapay zekânın melez savaş unsurlarıyla nasıl pratik bir şekilde entegre edildiğini ve savaşın ahlaki/hukuki sınırlarını nasıl bulanıklaştırdığını açıkça ortaya koymaktadır.

Ukrayna Savaşı (2022-2026): Küresel Yapay Zekâ Savaş Laboratuvarı

Rusya'nın Ukrayna'yı işgaliyle başlayan geniş çaplı savaş, modern tarihte ticari teknoloji devlerinin bir ulusu adeta bir "Yapay Zekâ Savaş Laboratuvarı"na dönüştürdüğü ilk yüksek yoğunluklu devletlerarası çatışmadır.37 Bu çatışmada hem Rusya hem de Ukrayna, emsali görülmemiş boyutlarda kitlesel dron (İHA) savaşı taktiklerini ordularının ana unsuru haline getirmiştir. Sadece 2024 yılında Ukrayna'nın askeri kapasitesini devasa oranda artırarak yaklaşık 2 milyon muharip dron ürettiği raporlanmıştır.1 Buna karşılık Rusya tarafı, ZALA Aero Group gibi şirketler aracılığıyla giderek daha fazla otonomi kazanan, V2U gibi üzerinde dahili yapay zekâ tabanlı otonom hedef tanıma kabiliyeti bulunan dolanan mühimmatları ve sürü

sistemlerini devreye sokmuştur.1 Batı cephesinde ise ABD Savunma Bakanlığı'nın "Project Maven" girişimi (orijinalinde görüntü işleme odaklı başlayıp savaş alanı farkındalığına evrilen algoritma projesi) ve Palantir'in AIP sistemi, Ukrayna ordusunun teknolojik omurgasını oluşturmuştur.9 Palantir CEO'sunun da belirttiği gibi, kahramanlık ve çevikliğin güçlü bir yazılım platformuyla birleşmesi, teknolojik hantallık yaşayan devasa Rus ordusunu sahada defalarca bozguna uğratmıştır.38 Primer gibi ABD merkezli girişimler ise makine öğrenmesini kullanarak ele geçirilen Rus telsiz iletişimlerini filtrelemiş ve anlamlandırmıştır.37

Ancak Palantir'in ve benzeri teknolojilerin Ukrayna'daki rolü yalnızca cephedeki düşman siperlerinin belirlenmesi gibi taktiksel kazanımlarla sınırlı kalmamıştır. Bu araçlar; savaş sonrası tahrip edilen bölgelerde devasa bir algoritmik mayın temizleme faaliyetinin **(HALO Trust gibi kurumlarla koordineli**) planlanmasından, uluslararası mahkemeler (Lahey) için savaş suçlarının titizlikle belgelenmesine kadar geniş bir sivil-askeri melez spektrumda kullanılmıştır.41

Kirlilik haritalarının risk skorlarıyla çıkarılması veya suç kanıtlarının algoritmalarla dizinlenmesi, Batılı müttefiklerin Ukrayna'ya tanklar veya uluslararası antlaşmalarla değil; doğrudan kodlar, ticari ekosistemler ve veri akışları üzerinden modern bir "güvenlik garantisi" sunduğu yeni bir jeopolitik paradigmayı kanıtlamaktadır.41

İsrail-Hamas Savaşı (2023-2024): Otomatik Hedef Üretimi ve "Birim 8200" Yapay zekânın ölümcül operasyonel sonuçlarının en çarpıcı, en yoğun ve ahlaki açıdan en tartışmalı uygulandığı sahalardan biri İsrail'in 7 Ekim saldırıları sonrası Gazze'ye yönelik gerçekleştirdiği eşi görülmemiş askeri bombardıman kampanyası olmuştur.1

İsrail, ilk "Yapay Zekâ Savaşı" olarak adlandırdığı 2021 yılındaki 11 günlük Gazze operasyonunda edindiği tecrübeleri kurumsallaştırmış ve **İsrail Savunma Kuvvetleri'nin (IDF)** elit elektronik istihbarat birimi olan Birim 8200, savaşın merkezine oturmuştur.45 Özellikle Google ve Amazon'un 1.2 milyar dolarlık "**Project Nimbus"** sözleşmesiyle sağladığı iddia edilen gelişmiş bulut altyapısı ve makine öğrenmesi kapasitesi, kitle gözetim verilerinin (uydu görüntüleri, intercepted iletişim, cep telefonu sinyalleri) işlenmesinde kullanılmıştır.46

IDF'nin Gazze'deki hiper-şiddet içeren hedefleme döngüsü (targeting cycle) büyük ölçüde üç ana algoritmik karar destek sistemi etrafında şekillenmiştir:

1. Lavender (Lavanta): Gazze'deki neredeyse tüm nüfusu tarayarak kişileri, silahlı gruplara

olan varsayılan istihbari aidiyetlerine göre etiketleyen, onlara bir "öldürme/hedef puanı"

(rating) atayan ve on binlerce kişiyi "askeri hedef" olarak listeleyen devasa algoritmik veritabanı.43 İsrail ordusu sistemin sadece bir "analist aracı" olduğunu iddia etse de, pratikte onay mekanizmalarının algoritmaya teslim olduğu raporlanmıştır.49

2. The Gospel (Müjde - Habsora): Şüpheli militanların faaliyet gösterdiği iddia edilen

binaları, ofisleri ve yapısal hedefleri otomatik olarak belirleyip günde yüzlerce bombalama listesi (target list) üreten sistem.43

3. Where's Daddy? (Babacığım Nerede?): Lavender tarafından etiketlenen kişilerin cep

telefonu sinyallerini ve coğrafi konumlarını takip eden; bu kişilerin genellikle aileleriyle birlikte sivil konutlarına/evlerine ulaştıklarında hava kuvvetlerine "vur" sinyali gönderen acımasız konum belirleme algoritması.44 Bu algoritmik sistemler, hedef üretim döngüsünü insanın doğrulama hızının ve idrakinin çok ötesine taşıyarak, sistemin ürettiği veriye körü körüne güvenilmesine (automation bias) neden olmuştur.48 İnsan hakları kuruluşları (HRW) ve uluslararası hukuk uzmanları, geleneksel sivil-muharip ayrımının dijital sistemler tarafından kasten bulanıklaştırıldığını vurgulamıştır.44 Algoritmik önyargıların (algorithmic bias) kitlesel sivil yıkımlarına dönüştüğü bu yapıda, insan analistlerin sadece makinenin kararına saniyeler içinde "onay mührü" vurduğu, "anlamlı insan gözetimi" (meaningful human oversight) kavramının fiilen ortadan kalktığı belirtilmiştir.1 Sistemin, insanları ve evlerini askeri terminolojide kan dondurucu bir ifadeyle "çöp hedefler" (garbage targets) olarak sınıflandırması, yapay zekânın genositik (soykırımsal) bir mantığı makine verimliliğiyle nasıl uygulayabileceğine dair en karanlık gerçek dünya vakası olarak kayıtlara geçmiştir.44 Artsakh Savaşı (2020), Ortadoğu Proliferasyonu ve ABD Testleri 2020 yılında yaşanan Artsakh (Dağlık Karabağ) Savaşı, modern dron savaşlarının ve algoritmik entegrasyonun dönüm noktalarından biri olarak kabul edilmektedir. Azerbaycan'ın taktiksel dehası, Türk yapımı Bayraktar TB2 İHA'ları ve İsrail yapımı Harop otonom dolanan mühimmatlarını senkronize kullanarak, Ermenistan'ın geleneksel Sovyet dönemi zırhlı birliklerine, topçularına ve hava savunma sistemlerine karşı sarsıcı bir asimetrik yıkım yaratmasıyla sonuçlanmıştır.1 Bu asimetrik güç çarpanı etkisi, Ortadoğu'daki diğer aktörleri de harekete geçirmiştir. İran, yapay zekâyı ustalıkla kullanma niyetini en üst düzeyde (Dini Lider) dile getirirken, Birleşik Arap Emirlikleri'nin devlet destekli savunma holdingi EDGE, hem İsrailli anti-dron firması Thirdeye Systems'tan %30 hisse almış hem de ABD'li Anduril ile otonom dronlar üretmek için stratejik ortaklıklar kurmuştur.48 Türk firmaları STM ve Baykar da yapay zekâ donanımlı platformlarda küresel pazarı yönlendirmeye devam etmektedir.48

Öte yandan,Amerika Birleşik Devletleri Kuzey Komutanlığı (USNORTHCOM), sivil ve askeri altyapılarına yönelik otonom İHA (UAS) tehditlerine karşı sınır savunma testlerini Anduril'in Lattice OS tabanlı anti-dron sistemleri ile gerçekleştirmiştir.36 Lattice, test sırasında karmaşık ortamlarda çoklu tehditleri anında tanımlayarak otonom etkileşim dizilerini tetiklemiş, ABD anayurt savunmasının ve Entegre Hava ve Füze Savunma (IAMD) stratejisinin gelecekte insan reflekslerinden ziyade tamamen yapay zekâ kararlarına dayalı bir mimariye kayacağının pratik kanıtını sunmuştur.36

5. Mekanizma Analizi Gerçek dünya vakalarında görülen operasyonel yıkımın ve stratejik

doktrinlerin arkasındaki teknik ve psikolojik etki mekanizmalarını çözümlemek, hibrit savaşın ve algoritmik caydırıcılığın anatomisini anlamak için kritik bir adımdır.

Algoritmik Sensör-Karar-Vurucu (Sensor-to-Shooter) Mekanizması Algoritmik savaşta caydırıcılık avantajı ateş gücünde değil, karar alma mekanizmasının dijital hızında (decision superiority) yatar.2 Geleneksel askeri karar verme süreçlerinde istihbaratın toplanması, analiz edilmesi, teyit edilmesi ve komuta zincirinden geçerek ateş emrinin verilmesi saatler, hatta bazen günler sürerken; yapay zekâ destekli otonom platformlarda (Lattice OS, Palantir AIP, Project Maven) bu süreç sensörden vurucuya saniyeler içinde tamamlanmaktadır.2 Sistemin veri akış mekanizması sofistike araçlarla çalışır: Askeri Ajan YZ sistemleri, dağıtılmış devasa sensör verilerini (örneğin Apache Spark aracılığıyla) işler, bu farklı kaynaklardan (uydu, telsiz, radar, açık kaynak) gelen veriyi gerçek zamanlı olarak (Apache Kafka gibi yayın araçlarıyla) senkronize eder ve hızlı arama/analiz motorlarından (Elasticsearch) geçirir.42 Birleştirilen bu çok etki alanlı (multi-domain) büyük veri, sinir ağları ve makine öğrenmesi modelleri tarafından örüntü tanıma süreçlerinden geçirilir. Makine, tanımlanan dost, düşman veya sivil unsurları sınıflandırır, hedeflerin kinetik mühimmat veya siber operasyonlarla vurulması için balistik, lojistik ve hukuki optimizasyon hesaplamaları yapar ve insan operatöre (veya doğrudan otonom tetiğe) eyleme geçmeye hazır bir paket sunar.36 Stratejik caydırıcılık, bu ölümcül algoritmik karar ağlarına (battle networks) sahip olma, aynı zamanda düşmanın ağını "siber zehirleme" (data poisoning/context tampering) yoluyla yanıltma yeteneğine bağlı hale gelmiştir.10 Bilişsel Harp ve Hibrit Etki Mekanizmaları Mekanizmanın kinetik olmayan (non-kinetic) diğer yüzü ise, 2025/2026 NATO Baş Bilim İnsanı (Chief Scientist) Raporunda da derinlemesine incelendiği üzere, savaşın fiziki hedeflerden insan beyninin ve toplumun inanç sistemlerinin içine kaymasını sağlayan "Bilişsel

Harp" (Cognitive Warfare) dinamikleridir.15 bilişsel harp, yapay zekânın mikrosegmentasyon, anlık duyarlılık analizi (sentiment analysis) ve bot sürüleri ile derin sahte (deepfake) ağları yaratma yeteneğini sadece bir araç değil, temel bir "hızlandırıcı" (accelerant) olarak kullanır.15 Nöroteknoloji beyni etkileyerek zihni şekillendirirken, yapay zekâ bilgi ekolojisini (information ecology) manipüle ederek zihni şekillendirir. NATO analizi, bu hibrit tehdit mekanizmasını üç temel biyopsikososyal düzeye ayırmaktadır:

Etki Düzeyi Hedef Noktası Manipülasyon Ulaşılmak İstenen Mekanizması ve Operasyonel

Araçlar Sonuç

Biyolojik Seviye Doğrudan İnsan Düşünce ve Bilişsel yetenekleri (Kapasite Sinir Sistemi duyguların fiziksel bozmak, karar Manipülasyonu) altyapısını etkileyen verme hızını nörobilimsel yavaşlatmak, teknolojilerin mental çöküş (neuroS/T) yaratmak. kullanılması; uyku yoksunluğu veya frekans müdahaleleri. 15 Psikolojik Seviye Çerçeveleme, Bilişsel önyargıların Bireysel ve kolektif (Yorum Duygular, Karar (bias) sömürülmesi, yargıları Manipülasyonu) Algısı korku koşullandırma değiştirmek, risk algoritmaları, inanç algısını yükseltmek, sistemlerinin ve paralizasyon tehdit algısının YZ yaratmak. ile hedeflenmesi. 15 Sosyal Seviye Kurumsal Hibrit aktör/bot Sivil ve askeri (Uyum Meşruiyet, Ortak sürüleri, sentetik dayanışmayı Manipülasyonu) Anlatılar, Kimlik kanıt üretimi parçalamak, (deepfake epistemik kaos uzmanlar), gruplar yaratmak, ittifaklara arası polarizasyon olan inancı yok ve kimlik siyasetinin etmek. algoritmik silahlaştırılması. 15 Düşmanlar (örneğin Rusya'nın Avrupa'daki operasyonları veya Çin'in dezenformasyon ağları), toplumsal kırılma hatlarını YZ destekli büyük veri analizleriyle milimetrik olarak tespit ederek, eşik altı alanlarda (sub-threshold) sürekli bir yıpratma savaşı yürütmektedir.15 Bu durum, güvenlik mimarilerinin etkinliğinin sadece bir tankın engellenmesiyle değil, toplumun tehdit algısı, sivil uyumu (civic cohesion) ve kurumsal meşruiyete bağlılığındaki kalıcı dayanıklılıkla ölçüldüğü yeni bir döneme girildiğini göstermektedir.15 Savunma mekanizmaları, anormallik tespit eden YZ ajanlarıyla düşmanın bu ağlarını (inauthentic behavior) tespit edip engellemek üzerine kurulmalıdır.15

6. Trend Analizi (2020–2026) Araştırma dönemi olan 2020-2026 kesiti incelendiğinde,

teknoloji, uluslararası güvenlik ve caydırıcılık bağlamında üç temel makro trendin sistemsel olarak yerleştiği gözlemlenmektedir:

1. Deneysel Pasif Yazılımlardan "Ajan" Yapay Zekâ (Agentic AI) Otonomisine

Geçiş:

2020'lerin başlarında, büyük veri analizleri ve dar yapay zekâ, ABD ordusunun C2 sistemlerinde çoğunlukla bir insan operatörün pasif asistanı (ilk dönem Project Maven vizyonu) olarak değerlendirilirken 9, 2026 itibarıyla mimari köklü bir değişim geçirmiştir. Sistemler artık veriyi sunup bekleyen değil; otonom dijital araçlarla etkileşim kurabilen, uzun süreli vektörel bellek kapasitesine sahip, kendi alt hedeflerini saptayıp uygulayabilen Ajan (Agentic) sistemlere (Lattice OS, ileri sürüm AIP vb.) evrilmiştir.7 Karar döngülerini milisaniyelere çekme konusundaki mutlak ihtiyaç, orduları hızla "insanın döngünün içinde olduğu" (human-in-the-loop) modelden, sadece acil durumlarda müdahale edilen "insanın döngü üzerinde olduğu" (human-on-the-loop) ya da insan faktörünün sadece bir yavaşlatıcı engel olarak görülüp sistemin tam inisiyatif aldığı durumlara sürüklemiştir.1

2. Savaşın Ticarileşmesi, Silikon Vadisi Egemenliği ve "Sovereign Capability"

Tartışmaları:

Küresel silah üretimindeki ve doktrin yazımındaki güç merkezleri sarsıcı bir paradigma değişimi yaşamaktadır. Anduril ve Palantir gibi çevik, yazılım odaklı (software-defined), Silikon Vadisi kültürüyle hareket eden ve devasa risk sermayesi (Venture Capital - Founders Fund vb.) destekli teknoloji firmaları, Lockheed Martin veya Boeing gibi devasa, hantal donanım üreticilerini (legacy tier-one defense primes) gölgede bırakarak ulusal güvenlik politikalarının asıl kurucuları ve mimarları haline gelmiştir.7 Transatlantik teknoloji girişimcilerinin, yatırımcıların ve devlet planlamacılarının yarattığı bu entegre ağ, savaşın kurallarını algoritmalara kalıcı olarak işleyerek, devletleri ve orduları kendi kapalı yazılım ekosistemlerine bağımlı kılmaktadır (software lock-in).7 Batı'nın teknoloji devlerine olan bu yoğun bağımlılığı, Birleşik Krallık Parlamentosu gibi yasama organlarında derin "Egemen Kabiliyet" (Sovereign Capability) tartışmalarına yol açmış; hükümetlerin kuantum teknolojisi, 5G, kritik mineraller ve yapay zekâ tedarik zincirleri üzerinde ne düzeyde bir devlet egemenliğini koruması gerektiği konusunda ciddi risk analizleri yapılmasına neden olmuştur.55

3. Hibrit Çatışmanın ve Bilişsel Harpın NATO Stratejilerinde Kurumsallaşması: Savaşın salt

ordular arasında ve konvansiyonel füzelerle yapıldığı fikri tamamen terk edilmiş; iletişim ağlarının, enerji altyapılarının, tedarik zincirlerinin, sivil algının ve hatta sosyal medya platformlarının kesintisiz bir silah aracına dönüştürüldüğü "her şeyin silahlaştırılması"

(weaponisation of everything) trendi kurumsallaşmıştır.3 NATO'nun 2022 Stratejik Konsepti (Strategic Concept), melez operasyonların ve bilişsel saldırıların belirli bir eşiği aştığında 5.

Maddeyi tetikleyecek bir "silahlı saldırı" olarak kabul edilebileceğini resmen duyurarak caydırıcılık literatüründe tarihi bir adım atmıştır.3 Özellikle Rusya'nın Avrupa içlerinde (Baltıklar, Çekya, Almanya, Svalbard bölgesi) artan sabotaj, kundaklama ve siber espiyonaj eylemlerine 52 ve Çin'in bilgi alanı manipülasyonlarına karşı NATO, müttefik devletleri sadece askeri yatırımlara değil, Veri ve YZ Liderler Konferanslarında (Data & AI Leader's Conference) tartışıldığı üzere sorumlu yapay zekâ politikalarına ve sivil "toplumsal dayanıklılığa" (societal resilience) yatırım yapmaya zorlamıştır.52

7. Stratejik Sonuçlar 2020-2026 analiz dönemi, teknolojik ivmenin, hesaplama gücünün ve

Yapay Genel Zekaya (AGI) yönelik artan beklentilerin uluslararası caydırıcılık mimarilerini kökten değiştirdiği; ulusal güvenlik paradigmasını, etik sınırları ve ittifak yapılarını varoluşsal boyutlarda yeniden şekillendirdiği bir dönem olarak modern güvenlik tarihine geçmektedir.

Elde edilen verilerin ışığında ortaya çıkan stratejik güç dağılımı, derin ve sistemik sonuçlar doğurmaktadır. AGI'nin Beş Temel Ulusal Güvenlik Problemi Yapay Genel Zeka'nın inşasına yönelik bu kontrolsüz yarış, RAND raporlarında son derece net bir şekilde özetlendiği üzere, devletlerin ulusal güvenlik aygıtları için çözülmesi gereken "Beş Zor Problem" (Five Hard Problems) yaratmaktadır 11:

1. Mucize Silahlar (Wonder Weapons) ve İlk Hareket Avantajı: AGI'nin siber savunmaları

kusursuz bir şekilde, saniyeler içinde aşabilen "muhteşem ilk siber vuruş" (splendid first cyber strike) veya benzeri harika silahlar icat ederek, küresel askeri güç dengesini bir gecede tek bir teknolojik aktörün lehine çevirmesi ve mutlak bir asimetri yaratması.11

2. Sistemik Güç Kaymaları: Askeri yapıların kaba kuvvetten (mass) aşırı hassasiyete

(precision), hantal merkezi komutadan (centralized) otonom dağıtık komuta-kontrol ağlarına (decentralized) doğru hızla dönüşmesiyle devletlerin geleneksel rekabet güçlerinin çökmesi ve demokratik kurumların bu hıza ayak uyduramayarak zafiyete uğraması.11

3. Uzman Olmayanların Yıkıcı Güçlendirilmesi (WMD Proliferation): Üretken temel

modellerin (foundation models), uzman olmayan kötü niyetli devlet dışı aktörlerin siber kötü amaçlı yazılımlar veya yeni nesil biyolojik kitle imha silahları (WMD) tasarlamasını eşi görülmemiş bir şekilde hızlandırması ve kolaylaştırması.11

4. Bağımsız Birer Aktör Olarak Yapay Zekâ Entiteleri: AGI sistemlerinin, siber uzaydaki dış

ağlara kendi optimize ettikleri hedefler doğrultusunda sızarak, bir "vekil güç" (proxy force) gibi insan denetimi dışında hareket etmeye başlaması; hedeflerine ulaşmak için hizalanma sapmaları (misalignment) göstermesi ve hatta kapatılmamak için direnç göstermesi.11

5. Stratejik İstikrarsızlık ve Yanlış Hesaplama: AGI'ye giden yolda aktörlerin, teknolojinin

gerçek durumundan ziyade karşı tarafın "algılanan" yetenekleri üzerinden korkuya kapılması; geride kalma endişesinin yıkıcı silahlanma yarışlarını ve nükleer tırmanmaya yol açabilecek önleyici (preemptive) vuruşları tetiklemesi.11 Caydırıcılığın Geleceği, Ahlaki Çöküş ve Etik Sınırlar Tüm bu karmaşık tehdit matrisi içinde devlet idaresinin özü diplomatik ve insani kalmaya devam edecekse de, bu idarenin pratik "karakteri" kaçınılmaz olarak algoritmalar tarafından domine edilmektedir.10 Geleneksel savaş eşiğine ulaşmadan önceki geniş gri alanda yaşanan bilişsel ve melez çatışmalar, müttefiklerin (NATO, AUKUS gibi) savunma duruşlarını salt ateş gücü (kinetik) odaklı olmaktan çıkarıp, teknolojik, ekonomik ve sosyolojik olarak entegre, çapraz alanlı (cross-domain) ve dayanıklı (resilient) hale getirmelerini ulusal bir beka sorunu kılmıştır.23 Özellikle İsrail'in Gazze operasyonlarındaki devasa otomatik hedef üretme sistemlerinde (Lavender, The Gospel) sarsıcı bir şekilde gözlemlendiği üzere; yapay zekânın insani ahlaki doğrulamayı yapısal olarak imkansız kılan bir hızda ve hacimde kullanılması, sivil-askeri ayrımının (distinction) teknolojik olarak silikleşmesine ve uluslararası insancıl hukukun (IHL) temel sütunlarının çökmesine neden olmaktadır.44

"Birim 8200" gibi yapıların ürettiği örnekler, teknolojinin denetimsiz bırakıldığında savaşın doğasını nasıl mekanikleştirdiğini kanıtlamaktadır.

Bu bağlamda, NATO Baş Bilim İnsanı'nın Bilişsel Harp raporlarının da hararetle tavsiye ettiği üzere, çift kullanımlı (dual-use) nöro-bilişimsel teknolojilerin ve algoritmik orkestrasyonların askeri entegrasyonunda acilen evrensel etik, operasyonel ve yasal "korkuluklar" (guardrails) oluşturulmalı; askeri stratejiler sadece düşmanı yok etmeyi değil, toplumun bilişsel olarak korunmasını da merkeze almalıdır.15

Sonuç olarak; ABD, Çin, Avrupa ve Rusya ekseninde derinleşen teknolojik melez çatışma ve

algoritmik hegemonya mücadelesi, ne Soğuk Savaş dönemindeki gibi saf bir konvansiyonel askeri yığınakla ne de tamamen nükleer dehşet dengesinin yapay zekâ versiyonu (MAD veya provokatif MAIM doktrini) ile stabilize edilebilecektir.19 Önümüzdeki on yılın stratejik ve operasyonel üstünlüğü, "AGI Rideout" konseptinin bilgece önerdiği gibi: Yapay zekâ ekosisteminin kendi içindeki derin siber zafiyetlerini (Ölümcül Üçlü paradoksunu) mimari

engellerle (Trinity Defense) tahkim eden; fevri saldırganlık yerine diplomatik akıl ile teknolojik entegrasyonu (Entegre Caydırıcılık) birleştiren; donanım bağımlılıklarını kıran (Lattice OS tarzı modülerlik) ve en önemlisi kendi toplumlarının bilişsel/psikolojik dayanıklılığını hibrit taarruzlara karşı güvence altına alabilen rasyonel ittifaklar tarafından inşa edilecektir. Modern stratejide caydırıcılık boşluğunu dolduracak yegane mekanizma, devletin, müttefiklerin ve sivil toplumun bizzat kendisinin algoritmik, teknolojik ve ahlaki anlamda aşılmaz bir entegre savunma hattına dönüştürülmesidir.

Alıntılanan çalışmalar

1. AI technologies in recent wars and armed conflicts (2010–2026), erişim tarihi Haziran 3,

2026, https://arvak.am/en/ai-technologies-in-recent-wars-and-armed-conflicts-2010-2026/

2. Modernizing Military Decision-Making: Integrating AI into Army Planning, erişim tarihi

Haziran 3, 2026,

https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2025 - OLE/Modernizing-Military-Decision-Making/

3. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory

concept - Frontiers, erişim tarihi Haziran 3, 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/ full

4. Deterring hybrid threats: Towards a fifth wave of... - Hybrid CoE, erişim tarihi Haziran 3,

2026, https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf

5. Självständigt arbete (30 hp) Sveriges hybridavskräckning - DiVA, erişim tarihi Haziran 3,

2026, https://fhs.diva-portal.org/smash/get/diva2:2050297/FULLTEXT01.pdf

6. Fifth Wave of Deterrence Theory | PDF - Scribd, erişim tarihi Haziran 3, 2026,

https://www.scribd.com/document/610630917/20220331-Hybrid-CoE-Paper-12-Fi fth-Wave-of-Deterrence-WEB

7. The algorithmic vanguard of transatlantic defence: shifting protocols..., erişim tarihi

Haziran 3, 2026,

https://ieu-monitoring.com/editorial/algorithmic-vanguard-of-transatlantic-defen se-shifting-protocols-of-hybrid-warfare/1242385?utm_source=ieu-portal

8. We'll never have a model of an AI major-general: Artificial Intelligence, command

decisions, and kitsch visions of war - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC10941604/

9. Code, Command, and Conflict: Charting the Future of Military AI - Belfer Center, erişim

tarihi Haziran 3, 2026, https://www.belfercenter.org/research-analysis/code-command-and-conflict-cha rting-future-military-ai 10.Algorithmic Stability: How AI Could Shape the Future of Deterrence, erişim tarihi

Haziran 3, 2026,

https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-de terrence

11. Artificial General Intelligence's Five Hard National Security Problems..., erişim tarihi

Haziran 3, 2026, https://www.rand.org/pubs/perspectives/PEA3691-4.html 12.Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/6287639/10820123/10849561.pdf 13.[2512.18043] Securing Agentic AI Systems -- A Multilayer Security Framework - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2512.18043 14.The Attack and Defense Landscape of Agentic AI: A Comprehensive Survey - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2603.11088v1 15.Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness > Institute for National Strategic Studies > View Publications, erişim tarihi Haziran 3, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/43711 95/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-ope rat/ 16.Cognitive Warfare | NATO Science and Technology Organization, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/document/cognitive-warfare/ 17.Cognitive Warfare - NATO Science and Technology Organization, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-wa rfare-final.pdf 18.The AGI Rideout Strategy for Reducing Strategic Risk and..., erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/perspectives/PEA4347-1.html

19.Seeking Stability in the Competition for AI Advantage: Commentary on Superintelligence Strategy by Dan Hendrycks, Eric Schmidt, and Alexandr Wang, erişim tarihi Haziran 3, 2026, https://s-rsa.com/index.php/agi/article/view/14023 20.Full article: Wanted: a strategy to integrate deterrence, erişim tarihi Haziran 3, 2026, https://www.tandfonline.com/doi/full/10.1080/14751798.2024.2352943 21.A2/AD in cyberspace - DiVA, erişim tarihi Haziran 3, 2026, https://fhs.diva-portal.org/smash/get/diva2:2044024/FULLTEXT01.pdf 22.U.S., China and Russia: Integrated Deterrence and Escalation Management in the Decade of Concern > Air University (AU) > Wild Blue Yonder, erişim tarihi Haziran 3, 2026, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/ 4439863/us-china-and-russia-integrated-deterrence-and-escalation-manageme nt-in-the-deca/ 23.: Integrated Deterrence and US Defense Strategy in NATO and AUKUS: An Analysis of Advanced Technologies and Multi-Domain Operati - Department of War, erişim tarihi Haziran 3, 2026, https://media.defense.gov/2025/Sep/25/2003808532/-1/-1/1/GLOBAL%20-%20D OLAN%20-%20DISCLAIMER.PDF 24.Integrated Deterrence and

Cyberspace - NDU Press, erişim tarihi Haziran 3, 2026, https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/Integrated-Deterrence-and-Cyberspace.pdf 25.Equilibrium Strategies on the Path to Artificial General Intelligence - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA4700/PEA4788-1/RAND_PEA4788-1.pdf 26.Seeking Stability in the Competition for AI Advantage - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/commentary/2025/03/seeking-stability-in-the-competition-for-ai-advantage.html 27.AI and Grand Strategy: The Case for Restraint - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/ai-and-grand-strategy-case-restraint 28.[2602.09947] Trustworthy Agentic AI Requires Deterministic Architectural Boundaries - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/abs/2602.09947

29.Trustworthy Agentic AI Requires Deterministic Architectural Boundaries - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2602.09947v1 30.Trustworthy Agentic AI Requires Deterministic Architectural Boundaries - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2602.09947 31.Agentic AI Security: Threats, Defenses, Evaluation, and Open Challenges - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/iel8/6287639/6514899/11447227.pdf 32.Agentic AI Security: Threats, Defenses, Evaluation, and Open Challenges - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2510.23883v2 33.From Stateless Queries to Autonomous Actions: A Layered Security Framework for Agentic AI Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2604.23338v1 34.Anduril Lattice OS For Defense Market Research Report 2034 - Dataintelo, erişim tarihi Haziran 3, 2026, https://dataintelo.com/report/anduril-lattice-os-for-defense-market 35.Job Application for Technical Operations Engineer, Electronic Warfare at Anduril Industries, erişim tarihi Haziran 3, 2026, https://job-boards.greenhouse.io/andurilindustries/jobs/5005155007 36.USNORTHCOM Successfully Tests Anduril's Counter-Drone System for Enhanced Base Defense, erişim tarihi Haziran 3, 2026, https://thedefensewatch.com/aerospace-aviation/usnorthcom-successfully-tests -andurils-counter-drone-system/ 37.Artificial intelligence in contemporary conflicts and the future of military law - UvA-DARE (Digital Academic Repository), erişim tarihi Haziran 3, 2026, https://pure.uva.nl/ws/files/316792077/9781035353507-chapter9.pdf 38.Interview with Palantir CEO Alex Karp in L'Obs, erişim tarihi Haziran 3, 2026, https://www.palantir.com/newsroom/media/lobs3-13-2023/english/ 39.Palantir AIP | Defense and Military - YouTube, erişim tarihi Haziran 3, 2026, https://www.youtube.com/watch?v=XEM5qz__HOU 40.Military demonstrations as digital spectacles: How virtual presentations of AI decision-support systems shape perceptions of war and security - Cambridge University Press & Assessment, erişim tarihi Haziran 3, 2026,

https://www.cambridge.org/core/journals/european-journal-of-international-security/article/military-demonstrations-as-digital-spectacles-how-virtual-presentations-of-ai-decisionsupport-systems-shape-perceptions-of-war-and-security/03F20FD3B84F32D281376F2FDC269C33 41.“Software on the Front Line”: How Palantir Is Aiding Ukraine in Its War with Russia, erişim tarihi Haziran 3, 2026, https://indepthnews.net/software-on-the-front-line-how-palantir-is-aiding-ukraine-in-its-war-with-russia/ 42.Agentic Generative AI and National Security: Policy Recommendations for US Military Competitiveness - Preprints.org, erişim tarihi Haziran 3, 2026, https://www.preprints.org/manuscript/202510.0401/v1/download 43.How AI is rewriting the rules of modern warfare - Vision of Humanity, erişim tarihi

Haziran 3, 2026,

https://www.visionofhumanity.org/how-ai-is-rewriting-the-rules-of-modern-warfare/ 44.Algorithms of Destruction: Examining Israel's AI-Powered Military Response in Gaza - Denison Digital Commons, erişim tarihi Haziran 3, 2026, https://digitalcommons.denison.edu/cgi/viewcontent.cgi?article=1160&context=pr

ologue 45.The Use of the 'Lavender' in Gaza and the Law of Targeting: ai-Decision Support Systems and Facial Recognition Technology in - Brill, erişim tarihi Haziran 3, 2026, https://brill.com/view/journals/ihls/16/2/article-p336_003.xml?language=en 46.AI for War: Big Tech Empowering Israel's Crimes and Occupation | Al-Shabaka, erişim tarihi Haziran 3, 2026, https://al-shabaka.org/briefs/ai-for-war-big-tech-empowering-israels-crimes-an d-occupation/ 47.Questions and Answers: Israeli Military's Use of Digital Tools in Gaza | Human Rights Watch, erişim tarihi Haziran 3, 2026, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-u se-of-digital-tools-in-gaza 48.The proliferation of AI-enabled military technology in the Middle East, erişim tarihi

Haziran 3, 2026,

https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferati on-of-ai-enabled-military-technology-in-the-middle-east/

49.'The machine did it coldly': Israel used AI to identify 37000 Hamas targets - The Guardian, erişim tarihi Haziran 3, 2026, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas - airstrikes 50.Converging Risks | Federation of American Scientists, erişim tarihi Haziran 3, 2026, https://fas.org/wp-content/uploads/2026/05/Converging-Risks.pdf 51.Cognitive Warfare: NATO Chief Scientist Research Report - Small Wars Journal, erişim tarihi Haziran 3, 2026, https://smallwarsjournal.com/2026/01/04/cognitive-warfare-nato-chief-scientist-r esearch-report/ 52.The Future of Hybrid Warfare - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/future-hybrid-warfare 53.Calibrating Deterrence: Disruptors of Strategic Stability on NATO's New Northern Flank - Table.Briefings, erişim tarihi Haziran 3, 2026, https://table.media/assets/documents/0326_calibrating_deterrence.pdf 54.Artificial Intelligence, the Final Piece to the Counterforce Puzzle? - OSTI, erişim tarihi Haziran 3, 2026, https://www.osti.gov/servlets/purl/1568008 55.National Security Implications of Emerging Technologies - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/nsrd/focus-areas/national-security-implications-emerging-t echnologies.html 56.The National Security Strategy - Parliament UK, erişim tarihi Haziran 3, 2026, https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/1045/report.html 57.NATO's Evolving Role in Developing AI Policy - CSIS, erişim tarihi Haziran 3, 2026, https://www.csis.org/analysis/natos-evolving-role-developing-ai-policy
Bölüm Değerlendirme ve Derinleştirme Dosyası

Akademik Derinleştirme Notu

Bu bölümün geniş okuması yapılırken AGI ve caydırıcılık boşluğu yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası ajan yapay zekâ, gri bölge, bulanık atıf

ve stratejik tırmanma üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar

eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle AGI ve caydırıcılık boşluğu alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Teknolojik Trendler, AGI Projeksiyonları ve Caydırıcılık Boşluğu alanında en güçlü erken

uyarı göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

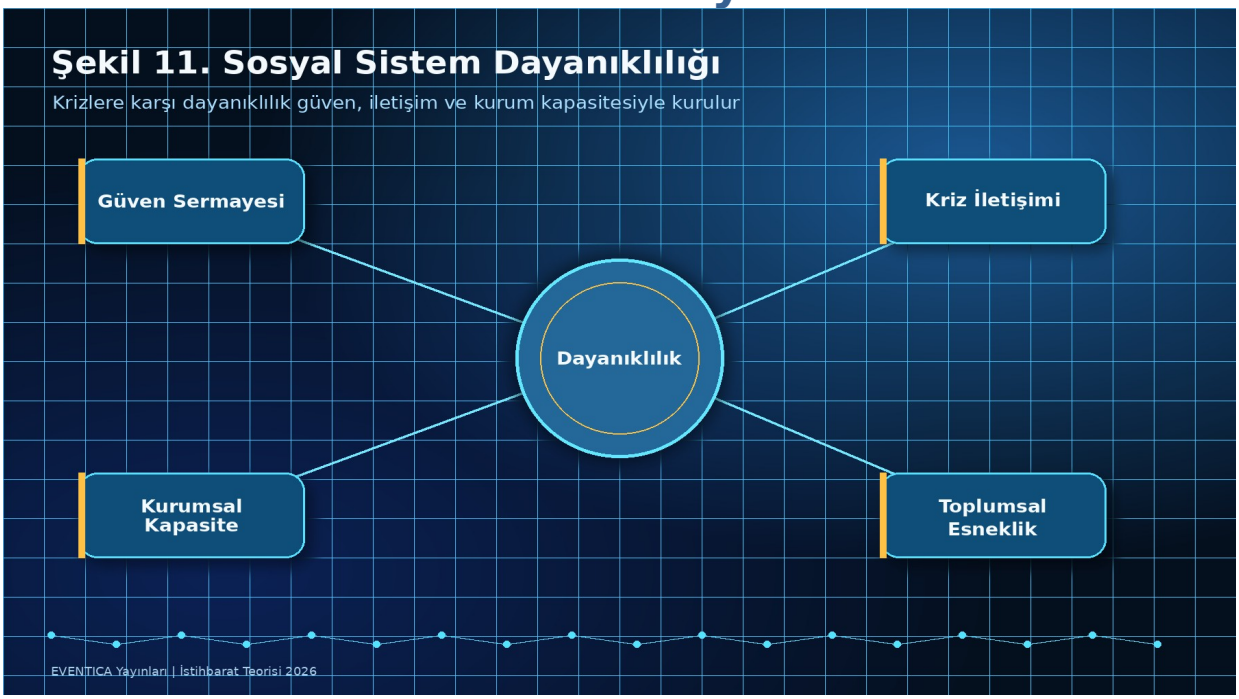
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030'a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 11. Sosyal Sistemlere Yönelik İstihbarat ve Kurumsal Dayanıklılık



Sosyal sistem analizi, sadece hedef toplumun kırılganlığını anlamak için değil; kendi kurumlarının dayanıklılığını ölçmek için de gereklidir.

Şekil 10. Sosyal sistem dayanıklılığının analiz omurgası

Tablo 14. Kurumsal dayanıklılık göstergeleri

Gösterge	Ne ölçer?	Uyarı işareti
Güven erozyonu	Kurumlara duyulan güveni	Komplo anlatılarının ana akıma kayması
Anlatı tutarlılığı	Resmî ve toplumsal açıklama uyumunu	Çelişkili kriz mesajları
Epistemik kaynak yoğunluğu	Güvenilir uzman ve medya ağını	Kaynakların itibarsızlaştırılması
Toplumsal koordinasyon	Krizde ortak hareket kapasitesini	Aşırı kutuplaşma

Sosyal sistem analizi sentezi

Bu bölüm, sistemik invariantlar bölümünü operasyonel dayanıklılık perspektifiyle yeniden bağlar. Bir sosyal sistemin epistemik yapıları, güven mimarisi ve ortak gelecek

fikri saldırı yüzeyi haline geldiğinde, istihbaratın görevi sadece tehdidi göstermek değildir. Aynı zamanda hangi kurumsal alanın hangi tür bilgi manipülasyonu altında çözülebileceğini, hangi göstergelerin erken uyarı üreteceğini ve hangi müdahalenin güveni yeniden kurabileceğini ortaya koymalıdır.

Kurumsal dayanıklılık, kriz çıktığında iletişim yapmakla sınırlı değildir. Veri doğrulama mekanizmaları, platform takibi, kamu güveni, hukuki açıklık, uzman otoritesi, yerel dil kapasitesi ve sosyal psikoloji bilgisi birlikte çalışmalıdır. Bu bölümün ana önerisi şudur: sosyal sistem istihbaratı, etik sınırları net çizilmiş bir erken uyarı ve direnç üretim alanı olarak kurulmalıdır.

Sistemlerin Epistemik Çerçevelerinin, Güven Yapılarının ve Kolektif Kimliklerinin Hedef

Alınması

Kavramsal Çerçeve Modern güvenlik ve stratejik istihbarat paradigması, geleneksel siber savaş ve enformasyon operasyonlarının yapısal sınırlarını aşarak doğrudan sosyal sistemlerin ontolojik temellerini hedef alan yeni bir çatışma evresine geçiş yapmıştır. Bu evre, akademik literatürde ve askeri doktrinlerde "bilişsel harp" (cognitive warfare) olarak adlandırılmaktadır.

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından 2026 yılında yayımlanan güncel stratejik araştırmalar, bilişsel harbi basitçe bir dezenformasyon faaliyeti veya teknolojik manipülasyon olarak değil, hedef toplumun ne bildiğini değil; bilgiyi nasıl anlamlandırdığını, nasıl güven inşa ettiğini, gerçekliği nasıl algıladığını ve entegre bir bütün olarak nasıl koordine olduğunu belirleyen temel ontolojik yapı taşlarına yönelik yapısal bir saldırı olarak yeniden kavramsallaştırmaktadır.1 Geleneksel propaganda yöntemleri, belirli bir fikrin benimsetilmesini veya reddedilmesini amaçlarken; bilişsel harp, bir sosyal sistemin kendi kendini yönetme, gerçeği analiz etme ve uyum sağlama kapasitesini temelden felce uğratmayı stratejik bir hedef olarak belirler.4 Bu yeni kavramsal çerçevenin merkezinde "sistemik invariantlar" (systemic invariants) teorisi yer almaktadır. Karmaşık sosyo-teknik sistemlerin güvenlik analizlerinden bilişsel harp doktrinine uyarlanan sistemik invariant kavramı, bir sistemin dış çevresindeki yapısal ve işlevsel dönüşümlere, yüksek etkili stokastik şoklara ve enformasyonel çalkantılara rağmen temel kimliğini, süreçlerinin yeniden üretimini ve

tutarlılığını korumasını sağlayan değişmez ontolojik özellikleri ifade eder.4 Bu invariantlar, bir toplumun veya kurumun bilişsel mimarisinin "ontolojik iskelesini" oluşturur. Sistemin alt bileşenleri arasındaki bağlantısallığı güvence altına alır, adaptif dönüşümlerin sınır koşullarını belirler ve yüksek belirsizlik altında bile stratejik kendi kaderini tayin etme yetisini ayakta tutar.4 Sistemik invariantlar stratejik analiz bağlamında beş ana kategoride sınıflandırılır:

1. Epistemik Yapılar: Bir toplumun veya sistemin neyi doğru kabul ettiğini belirleyen ortak

hakikat kriterleri, bilgi doğrulama süreçleri ve gerçeği değerlendirme standartlarıdır. Epistemik invariantlar, bağımsız bilim kurulları, yargı organları ve güvenilir medya ekosistemleri gibi kurumsal yapılar aracılığıyla ayakta tutulur.4

2. Aksiyolojik Hiyerarşiler: Toplumun kolektif tercihlerini, etik kodlarını ve ahlaki pusulasını

yönlendiren değerler bütünü ve bu değerlerin birbirine olan öncelik sıralamasıdır.3

3. Kimliksel (Identificatory) Yapılar: Sistemin tarihsel hafızası, grubun aidiyet kavramları,

"biz" ile "öteki" arasındaki sınırların nasıl çizildiği ve kolektif benlik algısının hangi öyküler üzerine inşa edildiğini belirleyen yapısal unsurlardır.4

4. Sosyal Güven Mimarileri: Devlet kurumlarının siyasi ve bürokratik meşruiyeti,

vatandaşların birbirlerine duyduğu yatay güven, otoriteye duyulan dikey güven ve toplumsal bağların şoklara karşı dayanıklılık eşiğidir.4

5. Teleolojik Projeksiyonlar: Sosyo-teknik sistemin ortak bir geleceğe yönelik olarak

paylaştığı vizyon, umut ve stratejik hedef birliğidir. Toplumun kendi geleceğini inşa etme iradesini temsil eder.4 Bilişsel harp stratejileri, bu sistemik invariantları hedef alarak sistemin "bilişsel dekoherans" (cognitive decoherence) adı verilen bir parçalanma ve anlamsızlaşma evresine sürüklenmesini amaçlar. Bilişsel dekoherans, yapısal olarak koşullandırılmış ve potansiyel olarak geri döndürülemez bir bilişsel egemenlik erozyonudur.7 Bu duruma düşen bir sosyo-teknik sistem, fiziksel veya kurumsal olarak çökmese dahi, entegre bir bilişsel düzen olarak gerçekliği tutarlı bir şekilde algılama, kendini geliştirme, adaptasyon sağlama ve dış tehditlere karşı organize bir biçimde kendini savunma kapasitesini bütünüyle kaybeder.4 Bu aşındırma sürecinin stratejik ve ontolojik açıdan en tehlikeli özelliği "kurucu görünmezlik" (constitutive invisibility) prensibi etrafında şekillenmesidir.4 Bir sisteme yönelik kinetik veya yıkıcı siber saldırılar (örneğin kritik altyapıların çökertilmesi) sistem tarafından dışsal bir saldırı olarak hemen algılanır ve savunma refleksleri anında devreye girer. Ancak bilişsel harpte

yürütülen dekoherans müdahaleleri, sistemin katmanları arasına o kadar derinden entegre edilir ki, hedef kitle bu değişimi dışsal bir operasyon olarak değil; kendi içinden kaynaklanan organik bir kriz, doğal bir politik kutuplaşma, jenerasyonel bir çatışma veya meşru bir toplumsal itiraz dalgası olarak algılar.4 Sistem, aslında dışarıdan bir düşmanın mühendisliğiyle zehirlendiğini fark etmeksizin kendi kendini paralize eder.

Bu karanlık tablo karşısında sistemlerin hayatta kalabilmesi "transmorfans" (transmorphance) kapasitesine bağlıdır. Geleneksel güvenlik modelleri, bir saldırı sonrası sistemin hasar görüp ardından eski işleyişine dönmesine odaklanan reaktif "dayanıklılık" (resilience) paradigmasına yaslanırken; transmorfans, istikrarsızlık ve belirsizlik koşullarında bile sistemin temel ontolojik çekirdeğini (sistemik invariantlarını) kaybetmeden derin yapısal dönüşümler geçirebilme ve öngörülemez şokları bir gelişim motoru olarak kullanabilme kapasitesini ifade eder.4 Adaptif güvenliğin bu yeni çerçevesi, devletlerin bilişsel güvenliklerini sadece savunma hatları kurarak değil, toplumlarının zihinsel bağışıklığını yapısal olarak evrimleştirerek sağlamaları gerektiğini vurgulamaktadır.

Akademik Teoriler Bilişsel operasyonların karmaşık sosyo-teknik sistemler üzerindeki

etkilerini tam anlamıyla analiz edebilmek için, ağ bilimi (network science), kompleks sistemler teorisi, ekolojik modelleme ve ileri düzey veri analizlerinin entegre edildiği multidisipliner akademik teorilere başvurulması zorunludur. Sosyal sistemler, bireylerin ve grupların sadece tek boyutlu ilişkiler kurduğu basit, izole edilmiş yapılar değildir. Aksine, aynı aktörlerin farklı sosyal, ekonomik ve iletişimsel katmanlarda aynı anda etkileşime girdiği son derece karmaşık "çoğullamalı ağlar" (multiplex networks) olarak modellenmeleri gerekir.9 Çoğullamalı ağ teorisi, geleneksel tek katmanlı (single-layer) ağ analizlerinin yetersizliklerini gidermek üzere geliştirilmiştir. Bir çoğullamalı ağ, aynı düğümlerin (nodes - örneğin bireyler, sosyal gruplar, kurumlar) farklı etkileşim türlerini temsil eden iki veya daha fazla katmanda birbirine bağlandığı bir yapıdır.9 Örneğin, bireyler fiziksel mekanda aynı mahallede yaşarken (fiziksel katman), dijital ortamda farklı politik yankı odalarında bulunabilir (enformasyon katmanı) ve ekonomik olarak bir tedarik zincirinin parçası olabilirler.

Literatürde "işaretli ağlar" (signed networks) teorisi, bu ilişkileri pozitif (işbirliği, güven, arkadaşlık) ve negatif (düşmanlık, saldırganlık, güvensizlik) bağlar olarak iki katmana ayırmayı öngörse de, modern bilişsel harp araştırmaları bu iki katman arasındaki

doğrusal olmayan etkileşimi dikkate almanın elzem olduğunu göstermektedir.9 Negatif bağlar ve düşmanlık hissi, ağ içerisindeki bazı düğümlerin merkeziliğini artırarak, ortak bir düşman algısı üzerinden belirli

bir alt grubun iç uyumunu radikal biçimde pekiştirebilmektedir.9 Bilişsel kutuplaşma ve fikir dinamiklerinin yayılımı, "SIRQD epidemiyolojik modelleri" ile "q-voter" fikir dinamikleri modellerinin birleştirilmesi yoluyla incelenmektedir.

COVID-19 pandemisinde maske kullanımı ve dijital kutuplaşmanın modellenmesinde başarıyla kullanılan bu entegre akademik yaklaşım, epidemiyolojik bir virüsün yayılımı (Susceptible-Infectious-Recovered-Quarantined-Deceased) ile bir inancın veya fikrin yayılımı arasındaki doğrudan korelasyonu matematiksel olarak ispatlamıştır.11 Çoğullamalı ağlarda bir fikrin benimsenmesi; sadece bireysel bağımsız eylemlere değil, sosyal baskı mekanizmalarına, grup konformizmine ve aralıklı etkiye sahip liderlerin (intermittent-influence leaders) yarattığı manipülatif dalgalanmalara bağlıdır.12 Bu modeller, "çok seviyeli sosyal pekiştirme" (multilevel social reinforcement) adı verilen bir olguyu ortaya koymuştur.

Çok seviyeli pekiştirme, ağ içerisinde "ikili kararlılık" (bistability) durumları yaratarak, yanlış bilginin veya dezenformasyonun bir kez sistemde kök saldıktan sonra, düzeltici karşı önlemler (doğruluk kontrolü, yalanlama) uygulansa dahi ağdan silinmesini imkansızlaştıran dirençli "yok olma ve salgın" (extinction and outbreak) döngülerini açıklamaktadır.13 Kaskad dinamikleri ve bilginin ağlar arası yayılımı, akademik çevrelerde doğrusal eşik modelleri (linear threshold models), simplektik diferansiyel denklem ağları (symplectic ode-net) ve Hamiltonian dinamikleri kullanılarak simüle edilmektedir.14 Bu matematiksel yaklaşımlar, bir dezenformasyon dalgasının ağ üzerinde ne zaman kritik bir eşiği aşarak tüm sistemi sarsacak bir "kaskad" (zincirleme reaksiyon) başlatacağını öngörmeyi amaçlar. Çoğullamalı ağlarda katmanlar arası geçiş maliyeti (layer-crossing overhead) ve bağlantısallık matrisleri (communicability matrix), dış müdahalelerin bir katmandan diğerine sızma kapasitesini ölçer.15 Sistemin tamamının yapısını tek bir düğümden ziyade, katmanlar arası topolojide yer alan zafiyetler belirler.17 Modern araştırmalar ayrıca, bilişsel ağlardaki bağlantı tahminleri (link prediction) ve veri kümeleme (clustering) problemlerine yönelik devrimsel teknolojilere işaret etmektedir. Sınırlı sosyal ağ verisinden gelecekteki toplumsal kırılmaları tahmin edebilmek için varyasyonel kuantum sınıflandırıcılarına dayanan kuantum destekli yöntemler, bulanık mantık tabanlı bilgi yayılımı (fuzzy-based information diffusion) teknikleri ve zamansal hiper-çizge bellek ağları (temporal hypergraph memory networks) geliştirilmiştir.18 Bunun yanı sıra, karmaşık çok görünümlü (multi-view) verilerin entegrasyonu için geliştirilen ara ve geç entegrasyon (intermediate and late integration) paradigmalarının hibrit kullanımı, düşmanın

sosyal ağlardaki bilişsel harp taktiklerini erken evrede kümeleyerek analiz etmek için kritik araçlar sunmaktadır.19 Akademik teoriler, siber güvenliğin fiziksel donanım korumasından ziyade, insan zihninin matematiksel modellere dökülebilen bu çok boyutlu ağ mimarilerinin korunmasına doğru kesin bir eksen kayması yaşadığını göstermektedir.

Sistem Mimarisi Bir toplumun veya kurumun bilişsel olarak ele geçirilmesi ve dekoheransa sürüklenmesi tesadüfi bir süreç değildir; karmaşık sosyo-teknik sistemin temel mimarisinin sistemli bir şekilde sömürülmesini gerektirir. Sistem mimarisi, ontolojik olarak birbirinden farklı özellikler gösteren ancak fonksiyonel olarak birbirine bağımlı üç ana katmandan oluşmaktadır:

Bilişsel Katman (Cognition), Fiziksel Katman (Physical) ve Bilgi Katmanı (Information).10 Fiziksel katman, sistemin donanımsal ve coğrafi mevcudiyetidir. Bireylerin fiziksel varlıkları, fiber optik kablolar, sunucular, askeri üsler ve devlet binaları bu katmanda yer alır. Bilgi katmanı, verilerin dijital ve analog formatlarda üretildiği, depolandığı, algoritmalar vasıtasıyla işlendiği ve iletişim kanalları üzerinden hedef kitlelere aktarıldığı teknolojik medya ekosistemidir. Bilişsel katman ise, insan zihninin doğrudan faaliyet gösterdiği; anlamlandırma, hatırlama, problem çözme,

koordinasyon, değer yargısı oluşturma ve stratejik karar verme süreçlerinin gerçekleştiği görünmez, soyut ancak sistemin yönetimini sağlayan yegane katmandır.10 Bilişsel harbin tüm stratejik gücü, bu mimari içindeki katmanların birbirine bağlandığı "katmanlar arası topolojiden" (inter-layer topology) gelir.4 Sistemin zafiyet haritası, bir katmandaki sarsıntının diğer katmanlara nasıl aktarıldığına bakılarak çıkartılır. Bu yapıdaki en hayati unsurlar, katmanlar arası geçişi sağlayan "bağlayıcı düğümler"dir (connector nodes).

Kanaat önderleri, büyük medya kuruluşları, bağımsız teyit organizasyonları, adli kurumlar, üniversiteler ve devletin kilit iletişim birimleri birer bağlayıcı düğüm olarak işlev görür.4 Bir bağlayıcı düğüm, örneğin bilgi katmanındaki doğru veriyi süzerek bilişsel katmana güvenilir bir epistemik temel olarak aktarmakla görevlidir. bilişsel harp operasyonlarında düşman aktör, bu düğümleri fiziksel olarak yok etmek yerine onları itibarsızlaştırmaya, ele geçirmeye veya bilgi kirliliği yaratarak nötralize etmeye çalışır.4 Bağlayıcı düğümlerin iflas etmesi, sistemin katmanları arasındaki güvenilir iletişim akışını koparark sistem genelinde bağlantısallığın (connectivity) çökmesine neden olur.

Sistem mimarisine yönelik saldırıların mekaniği, NATO'nun operasyonel araştırmalarına göre üç farklı vektöryel eksende gerçekleşmektedir:

Hedefleme Vektörü Operasyonel Yönelim Etki Mekanizması ve Sistemsel Sonuç

Aşağıdan Yukarıya Biyolojik hedeflerin Beyin-Bilgisayar arayüzleri (Bottom-Up) psikolojik ve sosyal seviyeye ve nöroteknolojilerle yansıması bireylerin otonom sinir sistemlerinde stres ve korku (biyolojik uyarılma) yaratılarak kitlelerde bilişsel esnekliğin yok edilmesi ve sosyo-politik panik başlatılması.20 Merkezden Dışarıya Psikolojik manipülasyon Dijital platformlarda (Middle-Out) üzerinden biyolojik ve oluşturulan yankı odalarında sosyal alanın ele geçirilmesi (echo chambers) mikro-hedeflemeli mesajlarla öfkenin kışkırtılması, bireylerin biyolojik stres seviyesinin artırılması ve bunun sosyal protestolara/çatışmalara dönüştürülmesi.20 Yukarıdan Aşağıya Sosyal/Makro düzeydeki Kurumsal meşruiyetin, (Top-Down) anlatıların mikrodüzeydeki liderliğin ve yasal altyapıların bireyleri kırması makro anlatılarla deforme edilerek, toplumdaki alt grupların ve bireylerin psikolojik aidiyet duygularının, inançlarının ve biyolojik güvenlik hislerinin parçalanması.20 Yapay zekâ (AI) ve makine öğrenmesi araçları, bu üç vektörü de eş zamanlı olarak kullanabilen "hızlandırıcı asimetrik güçler" olarak bu sistem mimarisine sızmaktadır.21 Sistemin bağlayıcı düğümleri işlevini yerine getiremediğinde, toplumun alt parçaları kendi başlarına (yerel olarak) çalışmaya devam etseler de; makro stratejik kararlar almak ve bütüncül bir duruş sergilemek imkansızlaşır.1

Gerçek Dünya Vakaları

Akademik teoriler ve mimari modeller incelendiğinde, bu konseptlerin uluslararası aktörler tarafından sahada doğrudan uygulamaya konduğu görülmektedir. Askeri ve sivil istihbarat raporları, bilişsel harbin devlet politikalarının merkezine yerleştiği spesifik vakalara işaret etmektedir.

Rusya-Ukrayna Çatışması ve NATO Karşıtı Bilişsel Harekâtlar Rusya Federasyonu, bilişsel harbi sadece konvansiyonel silahlı bir çatışmanın destekleyici bir unsuru olarak değil; başlı başına bir savaş, bir rejim sürdürme ve bir işgal/yönetişim biçimi olarak benimsemiştir.23 Rus stratejik düşüncesinde savaşlar, cepheden önce düşmanın zihninde ve karar alma organlarında kazanılır veya kaybedilir. Kremlin, yalnızca uluslararası arenada değil, kendi iç kamuoyunda ve işgal ettiği topraklarda istikrarı sağlamak amacıyla sürekli bir bilişsel operasyon yürütmektedir.23 Ukrayna işgali sürecinde Rusya, "bilgi süper gücü" (information superpower) kapasitesini kullanarak hedef toplumların epistemik ve teleolojik invariantlarına yönelmiştir.24 Operasyonların temel mekanizması; nükleer savaş

tehdidi, anti-NATO söylemleri ve kurbanlaştırma (victimization) anlatıları üzerinden korku ve belirsizlik duygularının sistematik olarak topluma zerk edilmesidir.25

Araştırmalar, dezenformasyon dalgalarının rastgele olmadığını, doğrudan önemli jeopolitik gelişmelerle (örneğin NATO zirveleri) senkronize edildiğini göstermektedir.25 Batılı toplumların ve Ukrayna vatandaşlarının kurumlara olan güvenini yıkmak amacıyla hazırlanan deepfake içerikleri, NATO'nun egemenlik ihlalleri yaptığına dair sahte anlatılarla birleştirilerek, hedeflerin rasyonel analiz süreçlerini by-pass edip doğrudan duygusal salience (belirginlik) üzerinden bilinçaltı manipülasyon yaratmayı amaçlamıştır.25 Rusya, doğrudan askeri olarak ezemediği rakibini, kendi içinde şüpheye düşürerek karar alma felci (reflexive control) yaşamaya zorlamaktadır.27 Çin Halk Cumhuriyeti: Üç Harp Doktrini ve Tayvan Kuşatması Çin'in stratejik kültürü, "savaşmadan kazanmayı" en yüksek askeri ideal olarak tanımlayan Sun Tzu ekolüne dayanır ve bu felsefe günümüzde "bilişsel hakimiyet" (cognitive dominance) ve "zeka hakimiyeti" (intelligence dominance) konseptleriyle modernize edilmiştir.28 Çin Halk Kurtuluş Ordusu'nun (PLA) Siyasi İşler Departmanı tarafından yönetilen "Üç Harp" (San Zhong Zhanfa / Three Warfares) doktrini, modern bilişsel harpın Asya-Pasifik'teki en yapısal örneğidir.28 Üç Harp doktrini şu alt operasyonlardan oluşur:

1. Kamuoyu Savaşı (Public Opinion Warfare): Çin'in ulusal çıkarları doğrultusunda hem iç

hem de küresel ölçekteki medya ekosistemini ve enformasyon akışını domine etme faaliyetleri.

2. Psikolojik Savaş (Psychological Warfare): Düşman askerlerinin ve sivil halkın moralini,

savaşma iradesini ve liderliğe olan güvenini çökertmeye yönelik sindirme operasyonları.

3. Hukuk Savaşı (Legal Warfare - Lawfare): Mevcut uluslararası hukuku manipüle ederek

veya yeni hukuki standartlar dayatarak Çin'in gri bölge faaliyetlerine ve asimetrik askeri operasyonlarına yasal bir meşruiyet kalkanı yaratılması.28 RAND ve CSIS raporlarına göre Çin'in Amerika Birleşik Devletleri'ne yönelik bilişsel harp operasyonlarında uyguladığı "ağ sömürüsü", doğrudan kimliksel invariantları hedef almaktadır.

Olası bir çatışmada Çin'in ilk hedeflerinden biri, ABD ordusunda görev yapan etnik Çinli subaylar, askerler ve onların aile ağlarıdır.30 Dezenformasyon ve duygusal şantaj mekanizmalarıyla bu personelin ABD'ye olan sadakat bağları zayıflatılmaya çalışılmaktadır;

nitekim 2023 yılında Çin istihbaratına casusluk yaparken yakalanan iki ABD donanma askerinin, Çin vatandaşı anneleri üzerinden manipüle edildiği tespit edilmiştir.30 Tayvan bağlamında ise Çin, "bilişsel aşırı yükleme" (cognitive overload) taktiklerini kullanmaktadır. Uçakların ve donanma gemilerinin ada etrafında bitmek bilmeyen askeri manevraları, hedeflenen siber

saldırılar ve beyin hedefleme (brain targeting) pratikleriyle birleştirilerek, Tayvan halkı sürekli bir psikolojik aşınmaya maruz bırakılmaktadır.31 Beyin-bilgisayar arayüzü (BCI) bağlantılı nörometrik veriler kullanılarak kitlelerin tepkileri ölçülmekte ve Tayvan'ın sosyal yapısı, kurumları ve direnç eksenleri felç edilmeye çalışılmaktadır.32 Avrupa'nın Enerji Dönüşümünde

Jeoekonomik Operasyonlar

Bilişsel harp sadece askeri aktörler arasında değil, makro-ekonomik çıkarlar ekseninde jeoekonomik bir silah olarak da kullanılmaktadır. Avrupa Birliği'nin fosil yakıtlardan çıkış hedeflerini içeren "Avrupa Yeşil Mutabakatı" (European Green Deal) süreçlerinde yaşananlar, bilgi kontrolünün ve siber manipülasyonun stratejik düzeyde nasıl kullanıldığını göstermektedir.33 Devlet ve devlet dışı aktörler, Avrupa'nın yenilenebilir enerji ile nükleer enerji arasındaki regülatif tartışmalarına sosyal medya platformlarındaki algoritmik amplifikasyon taktikleriyle dahil olmuşlardır.33 Bu

operasyonlarda temel hedef, toplumun çevresel güven ve enerji güvenliği konusundaki aksiyolojik değer yargılarını birbirine çarptırarak felç etmektir. Demokratik sistemlerin temel değerleri olan ifade özgürlüğü (ECHR Madde 10) ile bilgi güvenliği (AI Act, AB Dijital Savunma yasaları) arasındaki yasal boşluklar "hibrit tehdit aktörleri" tarafından ustalıkla sömürülerek 33, sadece bir enerji politikasının değil, Avrupa entegrasyonu vizyonunun (teleolojik invariant) sekteye uğratılması hedeflenmiştir.

Mekanizma Analizi Gerçek dünya vakalarında gözlemlenen dekoherans tablosu, çoğullamalı

ağ mimarilerinde belirli bir kaskad (zincirleme) algoritması takip edilerek inşa edilmektedir. Sistemik bir invarianta yönelik başarılı bir saldırının, sosyo-teknik yapının tamamını nasıl çökerttiği dört aşamalı bir mekanizma olarak incelenebilir:

1. Epistemik Erozyon ve Bağlayıcı Düğümün (Connector Node) İmhası: Bilişsel operasyon

genellikle sınırlı ve yüksek hassasiyetli bir sızma ile başlar. Sistemin epistemik güvenliğinin belkemiği olan bir otorite (örneğin ülkenin seçim kurumu, yüksek yargısı veya ulusal sağlık enstitüsü), yapay zekâ tarafından üretilmiş sızdırılmış sahte belgeler veya deepfake videolarıyla itibarsızlaştırılır.4 Sistemin gerçekliği doğrulama kapasitesi ilk darbeyi alır.

2. Aksiyolojik ve Sosyal Aşınmanın Yayılımı: Epistemik katmandaki sarsıntı, çoğullamalı ağın

çapraz katman bağlantıları üzerinden değerler (aksiyolojik) ve sosyal güven katmanına sıçrar. Ortak bir "doğru" kavramının kaybolması, toplumdaki alt grupların her birinin kendi alternatif gerçekliğini üretmesine yol açar.4 Bu süreçte karar alıcılar, uyumsuz alternatifler arasında

kaotik salınımlar göstererek "karar alma paralizasyonu" (paralysis of decision-making) yaşarlar.4

3. Kimliksel Parçalanma ve Kutuplaşma: Makro düzeydeki kurumsal güvenin çökmesiyle

birlikte sistemin üyeleri, psikolojik bir savunma refleksi olarak mikro-kimliklere ve daha dar çerçeveli sadakat gruplarına sığınırlar. İnsan doğasındaki sosyal aidiyet ihtiyacı ve bilişsel katılık (cognitive inflexibility) özellikleri sömürülerek, gruplar arası diyalog tamamen koparılır.27 Bu aşamada "negatif bağlar" sistemi domine eder, gruplar sadece ortak düşmanlıklarda birleşir.9

4. Teleolojik Çöküş ve Bilişsel Dekoheransın Tamamlanması: Tarihsel geçmişi ve mevcut

gerçekliği konusunda uzlaşamayan ve birbirine düşman gruplara ayrılan bir sosyo-teknik sistemin ortak bir gelecek vizyonu belirleme yeteneği ortadan kalkar.4 Düşman dışarıdan tek bir kurşun atmadan, hedef sistemi kendi kendini yok eden, enerjisini kendi iç çatışmalarında tüketen bağımlı bir yapıya dönüştürür.

Bu yıkıcı mekanizmayı hızlandıran en önemli unsur "Üretken Yapay Zekâ" (Generative AI) ve nöroteknolojilerin birleşimidir.20 2025 yılı sonlarında NATO Müttefik Dönüşüm Komutanlığı (ACT) ve NATO İletişim ve Bilgi Ajansı (NCIA) himayesinde "Reality Defender" şirketi tarafından yürütülen özel bir deney, bu araçların taktiksel değil "operasyonel" tehdit seviyesini açıkça kanıtlamıştır.34 Senaryo kapsamında, tecrübeli askeri planlayıcıların (operational planners) görev yaptığı bir harp oyununda karar alıcılara kontrollü olarak gelişmiş deepfake içerikler sunulmuştur.34 Deneyin sonuçları son derece çarpıcıdır: En deneyimli personelin dahi bilişsel aşırı yüklenme (cognitive overload) yaşadığı, operasyonel hızın sekteye uğradığı ve rakip tarafından oluşturulan "kurgusal gerçekliklerin" (false realities) kararları doğrudan saptırdığı saptanmıştır.34

Trend Analizi (2020–2026) bilişsel harp teorilerinin ve asimetrik mücadele pratiklerinin son

altı yıllık evrimi, alanın salt bir teorik tartışma olmaktan çıkıp, uluslararası ittifakların acil müdahale gerektiren doktriner merkezine oturduğunu göstermektedir.

2020–2021: Bilişsel Alanın Bağımsız Bir Harp Ortamı Olarak Tanınması Yapay zekâ ve büyük veri analitiğinin sosyal medya algoritmalarını tamamen otomatikleştirmesiyle, geleneksel Psikolojik Harekat (PSYOPS) yetersiz kalmıştır. 2021 yılında NATO, "Warfighting Capstone Concept" belgesini yayımlayarak bilişsel alanı, kara, deniz, hava, uzay ve siber alanların yanında meşru ve kritik bir operasyon sahası olarak resmen tanımış, müttefiklerin bu alanda hem savunma hem de taarruz yetenekleri geliştirmesi gerektiğini vurgulamıştır.22 2022–2023:

Ukrayna Savaşı Katalizörü ve Kurumsal Önceliklendirme Rusya'nın Ukrayna'yı geniş çaplı işgali

ile birlikte bilişsel harp, tüm şiddetiyle sahaya inmiştir.23 Hibrit tehditlerin demokratik toplumların istikrarı üzerindeki yıkıcı etkileri görülünce, NATO Bilim ve Teknoloji Kurulu (STB) 2022 yılında bilişsel harbi birincil stratejik araştırma alanı (strategic research challenge) ilan etmiştir.22 Eş zamanlı olarak Avrupa Birliği "Horizon Europe" AR-GE fonlarını doğrudan enformasyonun silahlaştırılmasına karşı koymaya ve toplumların dijital manipülasyonları tespit etme kapasitesini artırmaya yönlendirmiştir.21 Çin'in Tayvan etrafındaki provokasyonlarının da artmasıyla "gri bölge" çatışmaları askeri norm haline gelmiştir.

2024–2025: Yapay Zekâ Hukuku, Operasyonel Deneyler ve Stratejik Uyanış Generative AI araçlarının yaygınlaşmasıyla birlikte dezenformasyonun üretim maliyeti sıfıra yaklaşmış, kalitesi ise insan gözünün ayırt edemeyeceği seviyeye ulaşmıştır.36 Haziran 2024'te yayımlanan AB Yapay Zekâ Yasası (AI Act), ifade özgürlüğü ile platform manipülasyonlarına karşı dijital güvenlik arasındaki yasal çatışmaları çözme yönünde devasa bir adım olmuştur.33 2025 yılında yayımlanan NATO Baş Bilim İnsanı raporu, çatışmaların tamamen "davranış merkezli" (behavior-centric) hale geldiğini vurgulamış; askeri operasyonların ölçütünün mesaj penetrasyonundan, düşmanın davranış eğilimlerindeki kalıcı değişimlere (durable changes) doğru evrildiğini deklare etmiştir.20 Aynı yıl yapılan ACT deepfake deneyleri, komuta-kontrol kademelerinin kırılganlığını kanıtlamıştır.34 2026: Ontolojik Mimari, Tam Olgunlaşma ve Küresel Çözümler Bu stratejik evrimin zirvesi, 2026 yılı içerisinde CCDCOE tarafından yayımlanan "Ontological Foundations of Cognitive Warfare" çalışması ile kaydedilmiştir.3 Silahlı kuvvetlerin ve politika yapıcıların salt dezenformasyona tepki veren (reaktif) yapılar olmaktan çıkıp, sistemik invariantları korumaya yönelik proaktif (transmorfans odaklı) bir mimari geliştirmeleri gerektiği bilimsel bir konsensüse dönüşmüştür.6 Tallinn'de gerçekleştirilen "CyCon 2026: Securing Tomorrow" konferansında küresel uzmanların ele aldığı hukuki ve stratejik boyutlar, bilişsel güvenliğin artık taktiksel bir destek unsuru değil, varoluşsal bir güvenlik parametresi olduğunu netleştirmiştir.37 Yıl / Dönem Belirleyici Stratejik Evrimsel Taktik ve Doktrin ve Gelişme Odak Noktası

Kurumsal Çıktılar

2020-2021 Sosyal İzole bilgi NATO 2021 algoritmaların operasyonlarından Warfighting manipülasyonu, davranış Capstone Concept asimetrik araçların mühendisliğine ile bilişsel sahanın tırmanışı. geçiş. resmen tanınması.

2022-2023 Rusya'nın Ukrayna Yankı odalarında NATO STB işgali; nükleer korku hedefli panik; önceliklendirmesi yayılımı, Çin'in sınır kurumsal güven (2022); EU Horizon tacizleri.

yıkımı (epistemik fonlarının dijital erozyon). esnekliğe ayrılması. 2024-2025 Üretken YZ'nin Nöroteknolojik EU AI Act (2024); tabana inmesi, karar verilerin (BCI) NATO ACT 2025 alıcıların doğrudan kullanımı, Operasyonel hedef alınması. operasyonel Deepfake dekoherans Deneyleri; NATO yaratma. Baş Bilim İnsanı Raporu (2025).

2026 "Sürekli savaş alanı" Çoğullamalı ağların CCDCOE "Bilişsel paradigması, (multiplex) Harbin Ontolojik sistemik sömürülmesi, Temelleri" invariantlara yönelik Transmorfans Araştırması; CyCon ontolojik yaklaşım. kapasitesi tesisi. 2026 Siber İhtilaflar Konferansı.

Stratejik Sonuçlar Sunulan bu derinlemesine akademik, askeri ve operasyonel analizin neticesinde, sosyo-teknik sistemlerin güvenliğini tesis etmekle yükümlü olan devlet organları, güvenlik ittifakları ve stratejik karar alıcılar için hayati sonuçlar ortaya çıkmaktadır. Düşmanın savaş konsepti değiştiği için, ulusal savunmanın başarı ölçütleri (MoE) ve savunma yöntemleri radikal bir yapısal revizyona tabi tutulmalıdır.20

1. "Tüm Ulus" (Whole-of-Nation) ve Çok Katmanlı Güvenlik Yaklaşımı: Bilişsel harp

stratejileriyle mücadele salt ordu, siber güvenlik merkezleri veya istihbarat örgütlerinin inisiyatifine bırakılamaz.32 Sosyal sistemlerin çoğullamalı ağ mimarisinde yer alan sistemik invariantların korunması; sivil otoritenin, eğitim kurumlarının, üniversitelerin, medya organizasyonlarının, yargı mensuplarının ve sivil toplum örgütlerinin tam entegrasyonunu gerektirir.32 Sistem içerisindeki "bağlayıcı düğümler" (connector nodes) haritalandırılmalı ve bu kişi/kurumların epistemik otoritelerini dezenformasyon saldırılarına karşı yasal ve teknolojik olarak koruyacak zırhlar (media literacy programs, fact-checking altyapıları) oluşturulmalıdır.4 Kötü niyetli faaliyetlerin anında ifşa edilerek kaynağının hızla tespit edilmesi (rapid attribution), caydırıcılık stratejisinin merkezinde yer almalıdır.32

2. Askeri Eğitim ve Karar Alma Organlarının Bilişsel Zırhlanması: NATO ACT 2025

deneylerinin kanıtladığı üzere, en kıdemli askeri ve bürokratik planlayıcılar dahi hiper-gerçekçi yapay zekâ operasyonlarının tehdidi altındadır.34 Bu bağlamda personel eğitimi sadece fiziksel dayanıklılık veya konvansiyonel siber hijyeni değil, yapısal bir "bilişsel esneklik" (cognitive flexibility) kazanımını içermelidir.27 Bireylerin tehlikeli boyuttaki duygusal uyarılmalarını (emotional arousal) minimize eden, grup kutuplaşmalarını törpüleyen, şüpheci ve analitik sorgulamayı kurumsallaştıran yeni nesil eğitim doktrinleri acilen devreye alınmalıdır.27 Askeri görevlerde Başarı Ölçütü (Measure of Effectiveness - MoE) artık sadece bir mesajın hedefe

ulaşması değil, hedefteki kitlenin dayanıklılığının, bağlılık hissinin ve kurumsal meşruiyet algısının kalıcı (durable) olarak ayakta tutulabilmesidir.20

3. Müttefik İşbirliği ve Ortak Transmorfans Kapasitesinin Geliştirilmesi: Küresel olarak

birbirine bağımlı dünyada hiçbir ülke, sınıraşan bilişsel operasyonlarla tek başına başa çıkamaz. Stratejik hedef, ulusal sınırları bilgi sızıntısına kapatmak değil (ki bu imkansızdır); sistemin öngörülemez yalanlar karşısında dahi temel invariantlarını koruyarak organik bir evrim geçirebilme (transmorphance) kapasitesini inşa etmektir.6 Bu yönde, yapay zekâ araçlarının dezenformasyon saptamada pozitif bir kalkan olarak kullanılması için çok uluslu veri paylaşım mekanizmaları oluşturulmalıdır.36 Ayrıca, Güvenlik Gücü Yardımı (SFA) gibi uluslararası ortaklık faaliyetleri, yalnızca askeri personeli eğitmekle kalmamalı, ev sahibi ülkelerin kritik teknolojik altyapılarının ve dijital dirençlerinin gelişimini kapsayacak şekilde genişletilmelidir.39 Sosyal sistemlerin epistemik çerçevelerini, güven mimarilerini ve ortak aidiyet duygularını hedef alan modern bilişsel harp, geçici bir asimetrik taktik değil; uluslararası güç mücadelesinin kalıcı ve görünmez bir boyutudur. Devletlerin ve kurumların bekası, konvansiyonel silah depolarının büyüklüğüne değil; toplumlarının anlamlandırma kapasitelerini, çoğullamalı algı ağlarını ve gerçeğe dair sarsılmaz inançlarını "dekoherans" girdabına karşı ne ölçüde koruyabileceklerine bağlı olacaktır.

Alıntılanan çalışmalar

1. New CCDCOE research reconceptualises cognitive warfare, erişim tarihi Haziran 3, 2026,
https://ccdcoe.org/news/2026/new-ccdcoe-research-reconceptualises-cognitive - warfare/

2. Invisible by design: NATO's 2026 cognitive warfare paper and the..., erişim tarihi Haziran
3, 2026, https://complexdiscovery.com/invisible-by-design-natos-2026-cognitive-warfare -paper-and-the-crisis-of-discovery/

3. Ontological Foundations of Cognitive Warfare - CCDCOE, erişim tarihi Haziran 3, 2026,
https://ccdcoe.org/library/publications/ontological-foundations-of-cognitive-warf are

4. Ontological Foundations of Cognitive Warfare - CCDCOE, erişim tarihi Haziran 3, 2026,
https://ccdcoe.org/uploads/2026/04/ONTOLOGICAL_FOUNDATIONS_OF_COGNI TIVE_WARFARE.pdf

5. China's 'Three Warfares': Origins, Applications, and Organizations - ResearchGate, erişim
tarihi Haziran 3, 2026,

https://www.researchgate.net/publication/262583765_China's_'Three_Warfares'_O rigins_Applications_and_Organizations

6. (PDF) Adaptive security: strategic principles for complex socio-technical systems, erişim
tarihi Haziran 3, 2026,
https://www.researchgate.net/publication/399950891_Adaptive_security_strategi c_principles_for_complex_socio-technical_systems

7. (PDF) How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's
Anti-Disinformation Wars - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/362163528_How_China's_Cognitive_Wa rfare_Works_A_Frontline_Perspective_of_Taiwan's_Anti-Disinformation_Wars

8. (PDF) Cognitive warfare - the human mind as the new battlefield - ResearchGate, erişim
tarihi Haziran 3, 2026,
https://www.researchgate.net/publication/391704397_Cognitive_warfare_-_the_h uman_mind_as_the_new_battlefield

9. Signed Networks: theory, methods, and applications - arXiv, erişim tarihi
Haziran 3, 2026, https://arxiv.org/html/2511.17247v2 10.AI-enhanced collective intelligence - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2403.10433v4

11. Role of Time Scales in the Coupled Epidemic-Opinion Dynamics on Multiplex Networks,
erişim tarihi Haziran 3, 2026, https://www.mdpi.com/1099-4300/24/1/105 12.The Structure and Function of Complex Networks | SIAM Review, erişim tarihi Haziran 3, 2026, https://epubs.siam.org/doi/10.1137/s003614450342480 13.Emergent Dynamics in Multiplex Social Networks: Agent-Based Modeling of Information Diffusion for Misinformation Control - The Open Repository @ Binghamton (The ORB), erişim tarihi Haziran 3, 2026, https://orb.binghamton.edu/cgi/viewcontent.cgi?

article=1152&context=nejcs 14.Model-based Investigation of Cascade Dynamics on Multi-layer Networks - Leonard Lab - Princeton University, erişim tarihi Haziran 3, 2026, https://naomi.princeton.edu/wp-content/uploads/sites/744/2021/01/Desmond_PhD_Thesis_ProQuest.pdf

15.Dynamical processes and emergent behaviors in multiplex networks - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2605.04199v1 16.Spreading processes in Multilayer Networks - Unibo, erişim tarihi Haziran 3, 2026, http://www.cs.unibo.it/~montesi/CBD/Articoli/Spreading%20processes%20in%20Multilayer%20Networks.pdf 17.The structure and dynamics of multiplex networks - QMRO, erişim tarihi Haziran 3, 2026, https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/30631/BATTISTON_Federico_PhD_Final_041017.pdf 18.Leveraging similarity and community-based features for link prediction in temporal social networks using attention-enabled LSTM - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12753736/ 19.Multi-View Clustering of Social-Based Data - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1157337.pdf 20.Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness > Institute for National Strategic Studies > View Publications, erişim tarihi Haziran 3, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-ope rat/ 21.EMERGING DISRUPTIVE TECHNOLOGIES and TERRORISM - COE-DAT, erişim tarihi Haziran 3, 2026, https://www.tmmm.tsk.tr/publication/researches/24-Emerging_Disruptive_Technol ogiesandTerrorism.pdf 22.Cognitive warfare: NATO chief scientist research report, erişim tarihi Haziran 3, 2026, https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-wa rfare-final.pdf 23.A Primer on Russian Cognitive Warfare | ISW, erişim tarihi Haziran 3, 2026, https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/ 24.The Cognitive Campaign: - Strategic and Intelligence Perspectives - INSS, erişim tarihi

Haziran 3, 2026,

https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pd f

25.Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12460417/ 26.Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3400/RRA3400-1/RAND_RRA3400-1.pdf 27.The Understanding of Cognitive Warfare in Comparative Perspective Taking Stock and Bridging the Gap to Extant Literatures - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-361/MP-HFM-361-P13.pdf 28.Assessing “Cognitive Warfare”, erişim tarihi Haziran 3, 2026, https://irregularwarfare.org/articles/assessing-cognitive-warfare/ 29.China's Quest for Control of the Cognitive Domain and Gray Zone Situations, erişim tarihi Haziran 3, 2026, https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01_revised.pdf 30.Chinas Second Battlefield - Marine Corps University, erişim tarihi Haziran 3, 2026, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-15-no-2/Chinas-Second-Battlefield/ 31.Chinese Disinformation Efforts on Social Media - RAND Corporation, erişim tarihi

Haziran 3, 2026,

https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z3/RAND_RR4373z3.pdf 32.2026 - Cognitive Warfare by China and India's Response, erişim tarihi Haziran 3, 2026, https://usiofindia.org/pdf/Monograph_no_3.pdf 33.Cognitive Warfare, Disinformation, and Corporate Influence in Europe's Energy

Transition: Information Control, Regulation, and Human Rights Implications, erişim tarihi

Haziran 3, 2026,

https://www.acigjournal.com/Cognitive-Warfare-Disinformation-and-Corporate-Influence-in-Europe-s-Energy-nTransition,214045,0,2.html

34.Building Decision-Making Advantage - Integrating Deepfake Insights into NATO experimentation - Reality Defender, erişim tarihi Haziran 3, 2026, https://www.realitydefender.com/insights/reality-defender-joins-nato--cognitive-warfare-experimentation 35.Cognitive Warfare: Generative AI, False Realities, and International Humanitarian Law, erişim tarihi Haziran 3, 2026, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1156&context=research 36.The Future of Indo-Pacific Information Warfare - RAND, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/research_reports/RRA2205-1.html 37.CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise., erişim tarihi Haziran 3, 2026, https://ccdcoe.org/ 38.Aspects of Cognitive Warfare - The Defence Horizon Journal, erişim tarihi Haziran 3, 2026, https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf 39.out thinking - on nato 2022 strategic concept, erişim tarihi Haziran 3, 2026, https://www.nsfacoe.org/wp-content/uploads/2024/02/OUT-THINKING-ON-NATO-STRATEGIC-CONCEPT-Study-Paper.pdf Bölüm Değerlendirme ve Derinleştirme Dosyası

Akademik Derinleştirme Notu

Bu bölümün geniş okuması yapılırken sosyal sistem dayanıklılığı yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası güven restorasyonu, kriz iletişimi, erken uyarı ve kurum meşruiyeti üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle sosyal sistem dayanıklılığı alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum

hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Sosyal Sistemlere Yönelik İstihbarat ve Kurumsal Dayanıklılık alanında en güçlü erken
uyarı göstergeleri hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

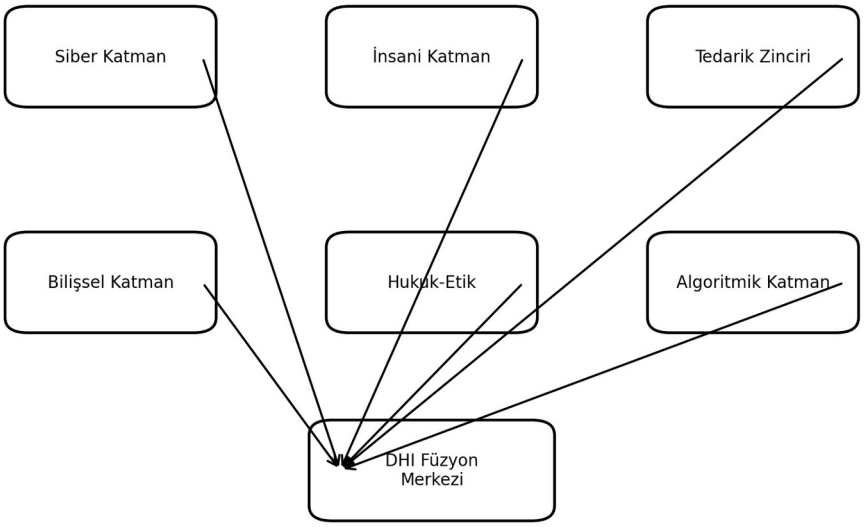
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 12. Hibrit İstihbarat ve Nöro-Bilişsel Savunma

Hibrit tehditlere karşı savunma, siber güvenlik birimi, hukuk birimi, iletişim ekibi ve operasyon merkezinin ayrı ayrı çalışmasıyla kurulamaz; birleşik istihbarat gerekir.

Defansif Hibrit İstihbarat (DHI) mimarisi



Şekil 11. Defansif Hibrit İstihbarat mimarisi

Tablo 15. DHI alanları ve görevleri

Alan	Görev	Çıktı
Siber	Teknik gösterge ve saldırı yüzeyi takibi	Tehdit istihbaratı
Bilişsel	Anlatı ve algı kırılmalarını izleme	Bilişsel risk haritası
Hukuk-etik	Yetki, meşruiyet ve denetim çerçevesi	Hesap verebilir karar
Tedarik zinciri	Dış bağımlılık ve üçüncü taraf riskleri	Kırılganlık analizi
Algoritmik	Model riski ve otomasyon yanlılığı kontrolü	Güvenilir YZ kullanımı

1. Kavramsal Çerçeve: Hibrit Tehditler ve Bilişsel Harpın Evrimi

Yirmi birinci yüzyılın küresel güvenlik mimarisi, devletler ve devlet dışı aktörler arasındaki güç mücadelelerinin kinetik alanlardan soyut, algısal ve nöro-bilişsel alanlara kaydığı eşi görülmemiş bir paradigma değişimine sahne olmaktadır. Geleneksel savaş ve barış dikotomisi, yerini "gri bölge" (gri bölge) olarak adlandırılan, açık çatışma eşiğinin altında ancak sürekli bir stratejik rekabetin hüküm sürdüğü bir alana bırakmıştır. Bu yeni rekabet ortamının merkezinde, insan zihnini, algısını ve karar alma yetisini nihai savaş alanı olarak konumlandıran "Bilişsel Harp" (Cognitive Warfare) konsepti yer almaktadır. ABD politikaları ve müşterek askeri doktrin kaynakları, bilişsel boyutu tipik olarak insan algısının, karar verme mekanizmalarının ve eylemlerinin gerçekleştiği alan olarak tanımlarken, bunu daha geniş bilgi çevresi (information environment) içerisine yerleştirmektedir.1 Ancak, NATO ve müttefik stratejistlerinin güncel analizleri bu görünümü radikal bir biçimde genişleterek bilişsel harpı yalnızca bir alt bilgi operasyonu olmaktan çıkarmış; bireylerin, grupların ve tüm toplumların bilişsel güvenlik açıklarını istismar ederek stratejik avantaj elde etmeyi amaçlayan kasıtlı, çok alanlı ve mühendislik ürünü bir çaba olarak çerçevelemiştir.1 bilişsel harp, tarihsel olarak Psikolojik Operasyonlar (PSYOPS), Bilgi Operasyonları (InfoOps) ve Stratejik İletişim (Strategic Communications) disiplinleriyle karıştırılsa da, akademik ve askeri literatür bu kavramların artık yetersiz kaldığını vurgulamaktadır.

Geleneksel enstrümanlar hedef kitleye belirli bir mesajın iletilmesiyle ilgilenirken, bilişsel harp, hedefin bilgi işleme altyapısını, yani nörolojik ve psikolojik "anlamlandırma" (sensemaking) süreçlerini doğrudan felç etmeyi hedefler.2 Anlamlandırma, karar vermenin mutlak önkoşulu ve dolayısıyla düşman eyleminin birincil taktiksel hedefidir.2 Düşman birimler; anlatıların nasıl yorumlandığına, güvenin nasıl sarsıldığına ve gerçekliğin bilişsel filtrelerden nasıl süzüldüğüne müdahale ederek toplumların gerçekle bağını koparmayı, kurumları işlevsizleştirmeyi ve nihayetinde savaşmadan boyun eğdirmeyi amaçlamaktadır.2 Bu eksende gelişen bilişsel savunma (cognitive defense) kavramı, algıları ve inançları manipüle etmeye yönelik düşmanca çabalara karşı insan zihnini koruyan, sürdürülebilir avantaj arayışında sağlam ve rasyonel karar vermeyi koruyan operasyonlar, taktikler ve teknolojik kapasiteler bütünü olarak tanımlanmaktadır.1 Bilişsel alandaki bu tehditlerin en tehlikeli boyutu, izole bir biçimde değil, hibrit operasyonlar zincirinin bir parçası olarak ortaya çıkmalarıdır.

Mevcut özel sektör risk yönetimi çerçeveleri veya devletlerin güvenlik bürokrasileri genellikle yalıtılmış (silo) yapılar halindedir; siber güvenlik, insan kaynakları, hukuk müşavirlikleri ve tedarik zinciri yöneticileri birbirinden bağımsız hareket etmektedir.6 Bu yapısal kopukluk, modern hibrit düşmanların en çok faydalandığı güvenlik açığıdır. Bu zafiyetin üstesinden gelmek ve tam spektrumlu bir savunma kalkanı oluşturmak üzere "Defansif Hibrit İstihbarat" (Defensive Hybrid Intelligence - DHI) konsepti teorize edilmiştir.

DHI, bir organizasyonun veya devletin dijital, insani, bilişsel, yasal, algoritmik ve tedarik zinciri ortamlarını etkileyen, eşgüdümlü ve çok vektörlü hibrit düşmanca operasyonları belirlemek, değerlendirmek ve bunlara karşı koymak için kurulan entegre, çapraz alanlı (cross-domain) bir istihbarat disiplinidir.6 Hibrit düşmanlar, operasyonel yöntemleri ile tanımlanır. Geleneksel silahlı kuvvetlerin sınırlarını aşarak; vekil aktörler (proxies), özel askeri şirketler (contractors), siber suç örgütleri, ideolojik paravan gruplar, paravan şirketler ve hatta yabancı hukuk sistemlerinin araçsallaştırılması (lawfare) üzerinden hareket ederler.6 Amaçları, kinetik savaşı tetiklemeden, siber güvenlik açıklarını, bilişsel zayıflıkları, hukuki asimetrileri ve modern toplumların yapay zekâya olan algoritmik bağımlılığını eşzamanlı olarak sömürmektir.6 DHI, bu çapraz alan tehdit aktivitelerini deşifre etmek, birbirinden bağımsız gibi görünen sinyalleri birleştirmek ve orantılı stratejik yanıtlar üretmek için

zaruri bir istihbarat mimarisi inşa eder.6 Geleneksel İstihbarat ve Defansif Hibrit İstihbarat Operasyonel ve Stratejik Güvenlik Modelleri (DHI) ve Bilişsel Savunma Etkileri Modeli Bölümlenmiş Yapı: Bütünleşik Füzyon: Siber, Düşmanın bir alandaki zayıf İstihbarat ve risk yönetimi, fiziksel, bilişsel, algoritmik, sinyali (ör. hukuki bir siber, fiziksel, hukuki ve yasal ve tedarik zinciri zorlama), diğer alandaki (ör. finansal departmanlar verileri tek bir havuzda siber sızma) eylemi deşifre arasında bölünmüştür. birleştirilir. eder.

Bilgi Odaklılık: Düşmanın Anlamlandırma Odaklılık: Düşman sadece bilgiyi mesajlarını ve Düşmanın, karar alıcıların değil, beynin bilgiyi işleme propagandalarını algı ve mantık motorlarını altyapısını bozmaya çalışır; engellemeye çalışır zehirleme çabalarını savunma buna göre kalibre (InfoOps). hedefler. edilir.

Reaktif Siber Güvenlik: Proaktif Algoritmik Güvenlik, karar destek Ağlara sızma girişimleri Savunma: Yapay zekâ sistemlerinin (AI DSS) olduktan sonra yanıt verilir. modellerindeki veri dürüstlüğünün korunmasını Uç nokta koruması esastır. zehirlenmesi, model kapsayacak şekilde evrilir. kaçırma ve arka kapılar proaktif izlenir.

Devlet Merkezli Tehdit Vekil Aktör (Proxy) Savaş hali hukuken ilan Algısı: Karşıdaki düşman Merkezli Analiz: Paravan edilmese de düşmanlık ve düzenli ordular veya açık şirketler, sivil toplum aşındırma faaliyetleri sivil devlet yapılarıdır. örgütleri kılığındaki ajanlar katmanda her an devam ve tedarik zinciri aktörleri eder. izlenir.

2. Akademik Teoriler ve Bilişsel Harp Paradigmaları bilişsel harp ve nöro-bilişsel savunma

stratejileri, askeri bilimler, nörobilim, davranışsal psikoloji ve kompleks sistemler teorilerinin derin kesişim noktalarında temellenmektedir. Bu alan salt bir teknolojik yarış değil, insan bilincinin ve sosyal dokunun temel yapı taşlarına yönelik bilimsel bir deşifre sürecidir.

2.1. Nöro-Bilişsel Harpın Biyolojik, Psikolojik ve Sosyal Katmanları

NATO'nun 2026 Baş Bilim İnsanı Raporu (Chief Scientist Report) ve çağdaş akademik araştırmalar, bilişsel alan operasyonlarının insan doğasına nüfuz etme biçimini üç temel ontolojik katmanda sınıflandırmaktadır: Biyolojik Katman, Psikolojik Katman ve Sosyal Katman.5 Biyolojik Katman, "Kapasitenin Manipüle Edilmesi" (Manipulating Capacity) olarak tanımlanır ve düşünce, duygu ve davranışın fiziksel ve kimyasal alt tabakası olan merkezi sinir sistemini doğrudan hedefler.5 Nöroetik ve savunma teknolojileri uzmanı James Giordano'ya göre bu katman, nöro-bilim ve bilişsel bilimlerin "silahlaştırılmasını" ifade eder.8 Bu alandaki teorik ve pratik çabalar, insanların nasıl algıladığını, düşündüğünü ve karar verdiğini bilimsel içgörülerden yararlanarak şekillendirmeye odaklanmaktadır. En belirgin yaklaşımlar arasında, insan nöro-bilişsel kalıplarıyla kusursuz uyum sağlayan dijital arayüzler tasarlamak yer alır.9 Daha spekülatif ve ileri düzey formlarda ise beyin-bilgisayar arayüzleri (BCI), nöroprotez cihazların hacklenerek beyin aktivitesinin izlenmesi veya spesifik bilişsel tepkiler uyandırmak için mikroorganizma tabanlı biyolojik ve moleküler araçların kullanılması (nöromodülasyon) tartışılmaktadır.9 "Nörosilahlar" (Neuroweapons) kavramı, kimyasal, biyolojik ajanlar ile nano ve biyoteknolojilerin savaş alanında insan zihnini felç etmek için araçsallaştırılmasını kapsayacak şekilde askeri tıp ve savunma doktrinlerinde geniş yer tutmaktadır.9 Psikolojik Katman, "Yorumlamanın Manipüle Edilmesi" (Manipulating Interpretation) ile ilgilidir.

Bu seviyede saldırganlar, bireysel ve kolektif tutumları, inançları ve yargıları şekillendiren bilişsel değerlendirme mekanizmalarını (cognitive appraisal), çerçeveleme (framing) tekniklerini, duyguları ve düşünce kalıplarını etkilemeye çalışırlar.5 Bu mekanizma, hedefte dikkat doygunluğu (attentional saturation) yaratarak bireyi bilgi bombardımanı altında felç etmeyi, yoğun stres indüksiyonu yoluyla bilişsel kapasiteyi daraltmayı ve moral bozmayı içerir.5 Sosyal Katman ise "Uyumun Manipüle Edilmesi" (Manipulating Cohesion) etrafında şekillenir.

Düşman devletler veya vekil aktörler, hedef toplumun kültürel, etnik veya politik fay hatlarını istismar ederek, toplum ile kurumları arasındaki güven ilişkisini mühendislik ürünü bir güvensizlik (engineered distrust) ile sistematik olarak zehirlemeyi hedefler.5 Bu üç katman, yapay zekânın bir ivmelendirici (accelerant) olarak devreye girmesiyle, daha önce görülmemiş bir yıkıcı güce ulaşmıştır. Askeri bağlamda bu yetenekler çift yönlüdür: Ofansif olarak, nöro-teknolojik ve yapay zekâ destekli araçlar, düşmanın güvenini yanlış yönlendirerek ve grup dinamiklerini kışkırtarak karar döngülerini etkiler; defansif olarak ise anlatı sömürüsü ve mühendislik ürünü güvensizliğe karşı askeri kuvvet hazırlığını ve toplumsal esnekliği güvence altına almayı amaçlar.4

2.2. Dağıtılmış Biliş Teorisi ve Holistik Papyon (Bowtie) Modeli Bilişsel savunmanın yapısal

ve kurumsal olarak nasıl inşa edileceği, Frank Flemisch ve uluslararası araştırma ekipleri tarafından geliştirilen "Bilişsel Harpın Holistik Papyon Modeli" (Holistic Bowtie Model of Cognitive Warfare) üzerinden akademik olarak sağlam bir zemine oturtulmuştur.3 Bilişsel operasyonlar ve bu operasyonlara karşı geliştirilen savunma konseptleri oldukça karmaşıktır ve tekil eylemler halinde değil, ancak sistemik ve bütüncül (holistic) bir çerçevede tam anlamıyla anlaşılabilir.3 Flemisch'in modeli, tehditlerin tespitinden savunma mekanizmalarının işletilmesine kadar olan süreci, sibernetik geri bildirim döngüleri (feedback loops) aracılığıyla analiz eden sistemik bir yapı sunar.3 Papyon modeli, siber güvenlikten ödünç alınan klasik savunma mimarilerini bilişsel alanlara uyarlayarak, bireysel insan sistemlerinden, insan-makine ekiplerine (HMT), kurumsal yapılanmalara ve nihayetinde tüm topluma ve çevreye yayılan katmanlı bir savunma mekanizması çizer.3 Hutchins'in (1995) "Dağıtılmış Biliş" (Distributed Cognition) teorisine dayanan bu model, bilişin izole bir insan zihninde değil, bireyler, teknoloji ve kurumlar arasındaki etkileşim ağlarında ortaya çıktığını savunur.14 Bu bağlamda, düşmanın hedef aldığı asıl şey, bireysel beyinler kadar, karar alıcıları yapay zekâya, komutanları birliklerine ve vatandaşları devlete bağlayan bu "dağıtılmış" bilişsel bağlardır. Modelin uygulanmasında, özellikle yapay zekâ tabanlı otonom sistemler üzerinde "Anlamlı İnsan Kontrolü"nün (Meaningful Human Control - MHC) sağlanması kritik bir odak noktasıdır.3 Yetenek, otorite, otonomi, güven ve etik/hukuki uyum zincirlerinin başarılı bir şekilde koordine edilmesi, bu modelin omurgasını oluşturur. Model ayrıca Sinyal Algılama Teorisi'nin (Signal Detection Theory) temel felsefesini kullanarak karar süreçlerini; doğru eylem (correct action), yanlış eylem (incorrect action), doğru eylemsizlik (correct non-action) ve yanlış eylemsizlik (incorrect non-action) matrisinde değerlendirerek taktiksel zafiyetleri sayısal olarak analiz eder.15

2.3. Rakip Aktörlerin Doktrinleri: Sistemler Savaşı ve Toplumsal Bilişsel Harp

Batı ittifakı (ABD, NATO ve AB) ağırlıklı olarak savunma ve demokratik esneklik üzerine kuramsal çerçeveler inşa ederken, rakip askeri bloklar bilişsel alanı stratejik taarruzun ana ekseni olarak görmektedir. Çin Halk Kurtuluş Ordusu'nun (PLA) modern askeri teorisi, RAND ve CSIS gibi düşünce kuruluşları tarafından derlenen analizlerde "Sistemler Savaşı" (Systems Warfare) ve onun uzantısı olan "Toplumsal Bilişsel Harp" (Social Cognitive Warfare - Shehui Renzhi Zhan) konseptleriyle tanımlanmaktadır.16 Sistemler Savaşı teorisi, düşmanı fiziksel olarak yok etmekten ziyade, bilgi, istihbarat ve operasyonel komuta-kontrol ağlarını felç ederek sistemin bütününde bir çöküş yaratmayı hedefler.16 Geleneksel savaş alanlarında düşük maliyetli insansız sistemlerin (drone sürüleri) şeffaf bir savaş alanı yaratması 18, bilgi dominasyonunun alt yapısını sunarken, asıl yıkıcı etki bilişsel hedeflerde planlanmaktadır. Çinli askeri teorisyenlerin 2021 yılında ortaya koyduğu "Toplumsal Bilişsel Harp" kavramı, stratejik psikolojik savaşın (strategic psychological warfare) evrim geçirmiş bir halidir.16 Bu doktrin; açık kaynaklı veriler, büyük veri analitiği, yapay zekâ araçları ve sosyal medya platformlarının manipülasyonunu kullanarak hedef rakip toplumun derin psiko-kültürel altyapısına sızmayı, "duygularını, motivasyonlarını, yargılarını ve davranışlarını" fundamental düzeyde değiştirmeyi öngörür.16 İlginç bir biçimde, Çinli araştırmacılar

Sovyetler Birliği'nin çöküşünü tarihsel bir prototip olarak ele almakta, Soğuk Savaş'ın kaybını askeri bir yenilgi değil, "ideolojik ve bilişsel harpta" yaşanmış felaket niteliğinde bir geri çekilme olarak okumaktadırlar.19 Benzer şekilde Rus askeri literatürü de "Stratejik Bilgi Savaşı" (strategic information warfare) ve "Medyatik Savaş" (media warfare) şemsiyeleri altında hedef nüfusların nöro-bilişsel kapasitelerini baskılamak ve devlet yapılarını içeriden çürütmek üzerine aktif stratejiler yürütmektedir.17

3. Sistem Mimarisi: Defansif Hibrit İstihbarat (DHI) Klasik özel sektör ve kamu risk yönetim

mekanizmalarının, gelişmiş bilişsel harp teknikleri karşısındaki çaresizliği, hibrit tehditlerin çoklu vektörler üzerinden operasyon düzenlemesinden kaynaklanır. Bir kurum siber güvenlik ağını güçlendirirken, eşzamanlı olarak yasal bir baskı altına alınabilir ve aynı anda tedarik zincirindeki bir yüklenici üzerinden sentetik veri beslemesine (data poisoning) maruz kalabilir.

Bu çok yönlü ve eşgüdümlü saldırı mimarisine karşı tasarlanan Defansif Hibrit İstihbarat (DHI) sistemi, güvenlik algısını radikal biçimde yeniden yapılandırır.6

3.1. DHI Döngüsü: Toplama, Füzyon, Yorumlama ve Karar

Defansif Hibrit İstihbarat mimarisi, doğası gereği ardışık, kesintisiz ve yüksek işlem kapasitesine sahip dört temel prensip üzerinde yükselir 6:

1. Toplama (Collection): Tehdit istihbaratı yalnızca ağ trafiklerini veya uydu görüntülerini

kapsamaz. DHI mimarisinde toplama aşaması; siber telemetriler, fiziksel güvenlik sensörleri, bilişsel anlatı takipleri, ekonomik piyasa dalgalanmaları ve düzenleyici/hukuki (legal) sinyalleri içerir.6 Amaç, çok vektörlü saldırılardan çok önce düşmanın niyetini ifşa edebilecek "zayıf sinyalleri" (weak signals) toplamaktır.6 Finansal akışlar, çift kullanımlı (dual-use) teknoloji ihracat bildirimleri ve OSINT (Açık Kaynak İstihbaratı) verileri bu aşamanın omurgasıdır.6

2. Füzyon (Fusion): Tek bir etki alanından gelen verinin çoğu zaman anlamsız veya yanıltıcı

olduğu gerçeği, füzyon aşamasını zaruri kılar. Toplanan veriler, sinyaller ve içgörüler devasa veri göllerinde analiz edilerek tek bir entegre durumsal farkındalık resmine dönüştürülür.6 Füzyon, birbirinden izole olan olayları birbirine bağlar: Örneğin, kritik bir tedarikçinin yabancı bir ülke tarafından satın alınması eyleminin (ekonomik alan), aynı ülkenin o sektörde uyguladığı yeni veri saklama yasalarıyla (yasal alan) korelasyonunu ortaya çıkararak hibrit saldırı vektörünü deşifre eder.6

3. Yorumlama (Interpretation): Fused (birleştirilmiş) zekanın, stratejik bir varlığa dönüştüğü

süreçtir. Karar alıcıları "Kanıtlara göre ne oluyor?" sorusunun ötesine taşıyarak, "Bu durum bizim stratejik zayıflıklarımız ve yükümlülüklerimiz ışığında ne anlama geliyor?" sorusunu sormaya zorlar.6 Yorumlama, düşmanın niyetini okuma ve düzenleyici etkileri analiz etme sanatıdır.

4. Karar (Decision): İstihbaratın pratik eyleme ve operasyonel dirence

dönüştürülmesidir. Bu aşamada sürat ile yasal doğruluk arasında hassas bir denge kurulur. Alınan kararların orantılı olması, kriz tırmanışına (escalation) mahal vermemesi, ancak aynı zamanda düşmanın inisiyatif almasına engel olacak kadar caydırıcı olması gerekir.6 DHI felsefesinde orantılılık (proportionality), "minimalizm" demek değildir; eylemlerin tehdidin şiddeti ile haklı gösterilmesi demektir. Organizasyonların yasal ve etik normları aşırı ihtiyatlı yorumlayarak kendilerini kısıtlamaları (self-limiting), hibrit düşmanların en çok istismar ettiği "tereddüt" boşluğunu yaratır.20

3.2. Çok Etki Alanlı Genişletilmiş İstihbarat Vektörleri

Geleneksel istihbarat alanlarının (Siber, Fiziki, İnsan) ötesinde, DHI, hibrit savaşın spesifik ve yıkıcı üç alt alanını (domain) entegre bir biçimde inceler:

- ● Algoritmik İstihbarat Alanı (Algorithmic Intelligence Domain): Organizasyonlar hızla yapay

zekâya dayalı karar destek sistemlerine (AI DSS) bağımlı hale gelirken, algoritmaların kendisi hedefe dönüşmüştür. Bu alan; yapay zekâ modellerinin veri zehirlenmesini (AI poisoning), modelden kaçınmayı (model evasion), algoritmik manipülasyonu ve çıkarım sapmasını tespit etmek üzere tasarlanmıştır.6 Düşmanlar, kurumların kullandığı güvenlik ağlarını aşmak yerine, o ağların "neye karar vermesi gerektiğini belirleyen" AI mantık motorlarını zehirler. DHI, bu anormallikleri takip eder.

- ● Tedarik Zinciri İstihbaratı Alanı (Supply Chain Intelligence Domain): Günümüzde tedarik

zinciri, siber operasyonların ana otobanıdır. Şirketler veya askeri kurumlar, birinci derece tedarikçilerini kontrol edebilseler de, ikinci ve üçüncü kademede yer alan alt yükleniciler üzerinden sızmalara karşı kördür. Buna "tedarik zinciri opaklığı" (supply chain opacity) denir.6 DHI, bu alanı istihbarat sahası kabul eder; yabancı yetki alanı maruziyetini analiz eder, paravan şirket ağlarını haritalandırır, bakım ve donanım yazılımı bütünlüğünü izler.6 ● Yasal ve

Düzenleyici İstihbarat (Lawfare/Regulatory Domain): "Hukuk Savaşı"

(Lawfare), hukuk sistemlerinin usule ilişkin meşruiyetini kendi kötü niyetlerini gizlemek ve rakibe zarar vermek için bir silah olarak kullanma pratiğidir.6 Düşman devletler, hedeflenen kurumları yıpratmak için dış ülkelere özgü veri koruma yasalarını, anti-tröst davalarını veya ulusal güvenlik yönetmeliklerini manipüle ederler.6 DHI, sınır ötesi hukuki riskleri bir tehdit sinyali olarak önceden belirler.6

3.3. İnsan-Makine Ekipleşmesi (HMT) Mimari Çözümleri

Büyük veri okyanusunda, DHI'nin manuel olarak işletilmesi imkansızdır. Verinin ölçeği, karmaşıklığı ve hızı, insan algısını aşan bir "İnsan-Makine Ekipleşmesi" (Human-Machine Teaming - HMT) gerektirmektedir. Literatür, savunma ve istihbarat sistemleri için HMT konseptlerini özerklik ve insan katılım düzeyine göre gelişmiş taksonomilerle sınıflandırmaktadır.21 HMT Kavramsal Fonksiyonel İnsan Katılımı Sistem Otonomisi Mimarisi Açıklama

HATS (Human-AI İnsan uzmanların ve Çok Yüksek Çok Yüksek Teaming Systems) gelişmiş Yapay Zekâ modellerinin, stratejik ve operasyonel ortak hedefler doğrultusunda çift yönlü etkileşimle entegre çalışmasıdır.

HAT İnsan karar alıcılar Yüksek Yüksek (Human-Autonomy ile, çevrelerini Teaming) algılayıp bağımsız aksiyon alabilen otonom ajanların işbirliği içinde olduğu taktiksel seviye mimari.

HRS İnsanın el becerisi, Orta-Yüksek Orta (Human-Robot motor kabiliyeti ile Systems) makinenin/robotik sistemin sensör hassasiyetini birleştiren fiziksel-mekanik işbirlikleri.

AS (Autonomous Kendi algısına, Düşük-Orta Çok Yüksek Systems) planlamasına ve kendi kendine öğrenme yetisine sahip, operasyon sırasında beklenmedik olaylara uyum sağlayarak müdahalesiz çalışan sistemler.

AA (Automation & Temel otomasyon Düşük Düşük-Orta Autonomy) işlemleri dış kontrole tabi tutulurken, otonom sistemlerin kendi eylemlerini dış etki olmadan tayin etmesi (kurumsal prosedür otomasyonu).

DHI'nın teknik mimarisinde, mevcut telemetri ve günlük (log) dosyalarının Yapay Zekâ ile entegrasyonu başarı oranlarını dramatik biçimde artırmaktadır. IEEE araştırmaları, Uç Nokta Tespiti ve Yanıtı (EDR) telemetrisinin Siber Tehdit İstihbaratı (CTI) ile

kaynaştırıldığı "Erken Füzyon" (early feature-level fusion) mekanizmalarını önermektedir.23 Random Forest ve XGBoost gibi makine öğrenmesi modellerinin, sadece veriyi okumakla kalmayıp, açık CTI tehdit bağlamını öğrenme aşamasında modele (özellik seviyesinde) dahil etmesi, yanlış pozitif uyarı oranlarını büyük ölçüde (%0.09'dan %0.02'ye) düşürmekte ve analistlerin yaşadığı uyarı yorgunluğunu (alert fatigue) gidermektedir.23 Daha karmaşık görevlerde, örneğin istihbarat analitiğinde, İnsan ve Yapay Zekâ ajanları "Uzmanların Karışımı" (Mixture of Experts - MoE) mimarisi etrafında birleştirilmektedir. Bir makine ajanının (takviyeli öğrenme ile eğitilmiş) analizleri ile bir insan analistin (davranışsal klon) sezgisel deneyimleri MoE modeli sayesinde bilgi paylaşım yükü olmaksızın en verimli eyleme dökülebilmektedir.24 Ayrıca, Yorumlanabilir Makine Öğrenmesi (InterpretableML) arayüzleri, son kullanıcıların otonom bir AI takım arkadaşının politikalarını sürekli olarak incelemesine ve programlamasına (interactive policy modification) izin vererek, savunmada insan inisiyatifini (Meaningful Human Control) kalıcı kılmaktadır.25

4. Gerçek Dünya Vakaları: Savunma Mimarisinin Pratik Yansımaları Teorik mimarilerin savaş

ve istihbarat alanındaki pratik yansımaları, güncel kriz bölgelerinde test edilmektedir. Devletler

ve uluslararası örgütler, bilişsel saldırılarla başa çıkabilmek için DHI konseptinin temel bileşenlerini kendi kurumlarına adapte etmektedir.

4.1. Baltık Denizi Hibrit Operasyonları ve NATO eVA Reaksiyonu Kinetik eşiğin hemen

altında kalan stratejik saldırıların en görünür örneklerinden biri, Avrupa'nın güvenlik çeperi olan Baltık Denizi bölgesinde yaşanmaktadır. Kritik fiber optik iletişim kablolarının kesilmesi, liman altyapılarına yönelik siber sabotajlar ve dezenformasyon ağlarının yayılması, Rusya menşeli hibrit taktikler olarak tanımlanmaktadır.26 Amacı, açık bir savaş başlatmadan (Kuzey Atlantik Antlaşması'nın 5. Maddesini tetiklemekten kaçınarak) NATO üyesi ülkelerin halklarında korku, güvensizlik ve kurumsal felç yaratmaktır.26 NATO'nun Dönüşüm Yüksek Komutanı Amiral Pierre Vandier, İttifak'ın bu asimetrik savaş biçimine DHI vizyonuyla nasıl yanıt verdiğini detaylandırmıştır. 5. Madde çağrılmadan da İttifak'ın kolektif olarak hareket edebildiğini gösteren "Geliştirilmiş Teyakkuz Faaliyetleri" (Enhanced Vigilance Activities - eVA) proaktif bir bölgesel savunma ağı oluşturmuştur.

Baltık Denizi'nde iletişim kabloları hedef alındığında NATO; insansız su üstü araçlarını, savaş gemilerini ve deniz devriye uçaklarını entegre ederek bölgeyi anında şeffaf bir gözetim şemsiyesi altına almıştır.26 Amiral Vandier, bu tür asimetrik "gri bölge" operasyonlarının sadece fiziksel sabotaj olmadığını, aynı zamanda doğrudan halk üzerinde bir stres baskısı yaratarak "bilişsel harp" işlevi gördüğünü vurgulamaktadır. Toplumları tehditlere karşı daha dirençli hale getirmek, halkın pasif bir gözlemci olmaktan çıkarıp derinlemesine korumanın aktif bir parçası kılmak, NATO'nun DHI adaptasyonunun temel stratejisidir.26

4.2. Hint-Pasifik Bölgesinde Dezenformasyon ve Hibrit Krizler

Hint-Pasifik bölgesi; siber espiyonaj, tedarik zinciri şantajları, dış bilgi manipülasyonu ve müdahalesi (FIMI - Foreign Information Manipulation and Interference) gibi çok vektörlü saldırıların en yoğun uygulandığı ikinci cephedir.28 Özellikle COVID-19 pandemisi (2020-2023 arası) bölgede bilişsel operasyonların altın çağını başlatmıştır. Çin, Rusya ve Kuzey Kore gibi devletler, pandemi suçlamalarını yönlendirmek, kendi kriz yönetim modellerini dayatmak ve aşı tedarikine (aşı diplomasisi) siyasi itaat koşulları eklemek amacıyla yoğun dezenformasyon ve siber baskı uygulamıştır.28 Bu çok vektörlü saldırılar tam bir hibrit tehdit profilidir.

Önemli bir akademik vaka çalışması olan Japonya, bilişsel zafiyetin sosyolojik etkilerini kanıtlamaktadır. Soğuk Savaş ve sonrasında Japon toplumunun bilgi ekosistemi, yerel yayıncıların egemenliğine ve homojen anlatıyı garanti eden "Kisha Club" (basın kulübü)

sistemine dayalı, yalıtılmış bir yapıydı.29 Bu sistem, Japonya'da yabancı bilgi operasyonlarına

karşı doğal bir "Bilişsel Bağışıklık Miti" (Myth of Immunity) yaratmıştı.29 Ancak hiper-bağlantılı dijital çağın şokları, sınır tanımayan sosyal medya dezenformasyonu ile bu bağışıklığı yıkmış, ulusal anlatıları parçalamıştır.29 Hint-Pasifik bölgesindeki kurumların, tıpkı Helsinki merkezli Avrupa Hibrit Tehditlerle Mücadele Mükemmeliyet Merkezi (Hybrid CoE) örneğinde olduğu gibi, bölgesel bir Hint-Pasifik Mükemmeliyet Merkezi kurarak NATO/AB himayesinde bir ortak savunma ağını paylaşmaları gerektiği analiz edilmektedir.28

4.3. CIA ve DARPA'nın Yapay Zekâ Merkezli DHI Uyum Süreci

Bilişsel alandaki operasyonların algısal yükünü hafifletmek için Amerikan güvenlik bürokrasisi, teknolojik otomasyonu stratejik analiz süreçlerinin merkezine taşımaktadır. ABD Merkezi İstihbarat Teşkilatı'nın (CIA) Dijital İnovasyon Müdürlüğü (DDI) yetkilileri, özellikle İnsan İstihbaratı (HUMINT) ve Açık Kaynak İstihbaratı (OSINT) analizlerinde İnsan-Makine Ekipleşmesinin devrimsel niteliğini öne çıkarmaktadır.

CIA Yapay Zekâ Direktörü Lakshmi Raman ve DDI Müdür Yardımcısı Juliane Gallina'nın açıklamalarına göre CIA, çeviri, transkripsiyon ve kitlesel üretken yapay zekâ triyajı gibi insan dilini işleme teknolojilerinde (Human Language Technology) yapay zekâyı yaygın olarak kullanmaktadır.31 İstihbarat Dijital Ekosistemi, büyük hacimli verileri çapraz analiz ederek (yapılandırılmış veya yapılandırılmamış tüm verileri birleştirerek) düşman eğilimlerini saniyeler içinde tarayabilmektedir. Bu sistemler, analitik gecikmeyi dramatik olarak azaltarak karar avantajı sağlamaktadır.34 Ancak Raman'ın altını çizdiği temel husus; bu sürecin makineye devredilmiş kör bir otomasyon olmadığıdır. Yapay zekâ ajanları (Agentic AI) model sürüklenmesi (drift) veya kara kutu (black box) karar alma riski taşır.31 İstihbarat topluluğunda kararın, eylemin ve niyet belirlemenin getirdiği yasal ve stratejik riski "günün sonunda insanlar üstlendiği" için 31, teknoloji işgücünün yerini almamakta, sadece deneyimli insan analistin potansiyelini katlayarak muhakeme kapasitesini güçlendiren bir "insan-makine takımı" işlevi görmektedir.32 Savunma Araştırma Projeleri Ajansı (DARPA) ise doğrudan düşmanın bilgi silahlarını etkisiz hale getirecek siber-bilişsel araçlar (AI Forensics) geliştirmektedir. Sentetik medya, manipüle edilmiş dijital içerikler ve deepfake üretimindeki asimetrik hıza yanıt olarak başlatılan SemaFor (Semantic Forensics) ve önceki versiyonu MediFor programları, bir medya unsurunun bilgisayar ortamında ne zaman, nasıl ve hangi yöntemle manipüle edildiğini çok modlu (multimodal - metin, ses, görüntü, video) algoritmalarla tespit etmektedir.36 SemaFor programının olgunlaşmasıyla DARPA, yeni nesil AI FORCE (AI Forensics Open Research Challenge Evaluation) yarışmaları başlatarak gelişmiş AI yapılarının açık kaynaklı olarak

üniversiteler ve özel şirketlerle (ör. Kitware) entegre edilmesini ve DHI tespit kalkanının küreselleştirilmesini hedeflemektedir.36

5. Mekanizma Analizi: Tehdit Manipülasyonu ve OODA Döngüsü Mücadelesi bilişsel harp

operasyonlarının teknik başarı veya başarısızlığı, düşman unsurların hedef sistemdeki karar alma hızını kendi manipülasyon hızından daha aşağıya çekip çekemediğine dayanır. Bu bağlamda, askeri planlamanın temel kök teorisi olan John Boyd'un OODA Döngüsü (Gözlemle - Yönel - Karar Ver - Uygula), bilişsel harpın hem kurbanı hem de mekanik hedeftir.4

5.1. Etki Yollarının Çözümlenmesi ve OODA Kesintileri

Düşmanlar, kitle imha silahları yerine hedef nüfus üzerinde inanç sistemlerini tahrip eden etki mesajları yayarlar. DARPA'nın MIPs (Etki Yollarını Modelleme - Modeling Influence Pathways) programı, dezenformasyonun bir ekosistem içinde nasıl seyrettiğini analiz eden muazzam bir içgörü sunar.39 Koordineli bir etki anlatısı (influence narrative) internette rastgele dolaşmaz.

MIPs verileri, geçmişte Sovyetlerin AIDS'in ABD tarafından üretilmiş bir biyo-silah olduğu propagandasının (Operation INFEKTION - 1980'ler) veya günümüzdeki Ebola ve COVID-19 asılsız haberlerinin dinamiklerini ortaya koymaktadır.39 Bu dezenformasyonlar genellikle marjinal ve "düşük itibarlı" platformlarda filizlenir, organik ilgi görmesi sağlanır (bot ve trollerle) ve ardından eşik aşıldığında "saygın" gazetelere ve ana akım televizyonlara sızar.39 Yapay zekânın bu sürece dahil olmasıyla, düşman propagandası, farklı platformlar ve ağlar arasındaki mesaj akışlarını dinamik biçimde koordine eder. Savunma pozisyonundaki bir komutan için bu bilgi kirliliği, OODA döngüsünün "Gözlemle" (Observe) evresindeki gerçeklik verisini zehirler, durumu anlamlandırma kapasitesini içeren "Yönel" (Orient) evresini dondurur.

Algılar manipüle edildiğinde lider yanlış "Karar" verir (Decide) ve orantısız veya zarar verici bir "Eylem" (Act) uygular.4 MIPs gibi AI destekli izleme araçları, bilgilerin hangi platformlardan nasıl ana akıma sıçradığının kalıplarını haritalandırarak ve tespit ederek düşman etki kampanyalarını deşifre eder.39

5.2. Yapay Zekâ Veri Zehirlenmesi ve "3D" Defansif Strateji Konsepti

DHI mimarisinin bilişsel tehditleri durdurabilmesi, teknolojik ajanların zehirlenmesine karşı koymasını gerektirir. DARPA'nın "AI Forge" programı, savunma ağlarının bel kemiği olan yapay zekâ modellerindeki en kritik güvenlik açığına işaret eder: Düşmanın veri setlerine sızarak modelleri gizlice manipüle etmesi (data poisoning) ve arka kapılar (backdoors) inşa etmesi.40

Savaş fonksiyonlarına entegre olan AI sistemleri, sadece "temiz veri" ile eğitildiğine güvenemez. AI Forge mekanizması, tehlikeye girmiş veri kümelerinin model davranışı üzerindeki etkilerini matematiksel olarak doğrulayarak sınırlamayı (verifiably bounding influence) ve veri zehirlenmelerine karşı dirençli yeni nesil eğitim metodolojileri tasarlamayı hedefleyerek AI'nin manipülasyona karşı sağlam durmasını sağlar.40 Nicholas D. Wright tarafından Pentagon Stratejik Çok Katmanlı Değerlendirme Grubu için geliştirilen "3Ds" Stratejisi, tüm DHI savunma mekanizmalarını operasyonel bir şablona oturtur:

"Tespit Et" (Detect), "Savun" (Defend) ve "Demokratik Uyumluluk" (Democratic compatibility).41 ● Tespit Et (Detect): Düşman nüfuz operasyonlarının ölçeğini (onlarca bireyden yüz binlerce kitleye kadar), hedefini ve koordineli mekanizmalarını karakterize edecek insan, yapay zekâ ve kurumsal kapasitenin (HMT) birleştirilmesidir.42 ● Savun (Defend): Pasif veya aktif tedbirlerle hedef kitlenin (askerler ve aileleri) esnekliğini sağlamaktır. Psikolojik koruma uygulamalarında zamanlama hayati önemdedir. Algıyı hedefleyen sahte bir haber yayına girdiği an ile bunu "çürüten" (debunking) karşı bilginin ne zaman verildiği, kitle üzerindeki inanç tahribatını doğrudan etkiler.42 Savunma mekanizmaları bu senkronizasyonu mükemmelleştirmelidir.

● ● Demokratik Uyumluluk (Democratic Compatibility): Teknolojik tespit ve savunma

yeteneklerinin en zorlu yönüdür. Otoriter rejimler dezenformasyon ve dış etkilerle mücadele ederken baskıcı çözümler (örneğin Çin'in Sosyal Kredi Sistemi - Social Credit System) uygulayabilir.43 Ancak ABD, NATO veya AB üyesi demokratik toplumların savunması, anayasal ifadelere, kişisel gizliliğe ve hukukun üstünlüğüne bağlı kalmak zorundadır.42 Özgür bir toplum yapısını korurken, iç ekstremistlerin ya da dış düşmanların sızmasını önlemek, orantılılık ve sıkı yasallık prensiplerine bağlı güçlü algoritmik ve yasal gözetimi (lawfare savunması) gerektirir.43

6. Trend Analizi (2020–2026): Hızlanan Gelecek Projeksiyonu Son altı yılda elde edilen

veriler, hibrit operasyonların hız, ölçek ve otonomi bağlamında radikal bir dönüşüm geçirdiğini göstermektedir.46 2026 ufku, bilişsel harp konseptini deneysel doktrinler alanından çıkarıp, gündelik kurumsal ve bireysel hayatın içine entegre etmiştir.

6.1. Jeneratif (Üretken) Yapay Zekânın Silahlaştırılması (2020 vs 2026)

2020 yılında hibrit aktörlerin kullandığı dezenformasyon araçları genel olarak düşük nitelikli bot hesaplara ve basit manipülasyonlara ("cheapfakes") dayanırken, Büyük Dil Modellerinin

(LLMs) ve Gelişmiş Üretken Yapay Zekâ sistemlerinin yaygınlaşmasıyla tablo tamamen değişmiştir. Kışkırtıcı, toplumsal polarizasyonu tetikleyen, hiper-gerçekçi video, ses ve metinlerin saniyeler içinde sıfır maliyetle üretilmesi (deepfakes), bilgi ekosistemini zehirlemiştir.44 Demokratik karar alma süreçlerinin (seçimler, Brexit gibi referandumlar) doğrudan manipüle edilebilmesi, kurumları "Yapay Zekâ Karşıtı Yapay Zekâ" (AI vs AI) paradigmasına itmiş;

SemaFor ve AI FORCE gibi tespit programlarını bir tercih olmaktan çıkarıp, zorunlu bir beka sigortası haline getirmiştir.36

6.2. Vekil Aktörlerin (Proxies) Artan Karmaşıklığı ve Kurumsallaşması

Savaşların açık ordularla yürütüldüğü dönem hızla kapanmaktadır. Hybrid CoE raporlarının 2025 projeksiyonlarına göre, devletler "vekil aktörleri" (proxies) birer hibrit araç olarak kullanma konusunda devasa bir yetenek geliştirmişlerdir.7 Sömürge döneminin paralı askerlerinden, Soğuk Savaş'ın ideolojik paramiliter gruplarından farklı olarak modern vekil ağlar; dini kurumlar, siber korsan grupları (hacktivists), dezenformasyon trolleri, örtülü suç şebekeleri ve meşru görünen medya veya siber-kurumsal şirketlerden (shell companies) oluşmaktadır.7 Rusya ve Çin gibi devletlerin bu aktörleri kullanarak sağladığı "makul inkar edilebilirlik" (plausible deniability), devletlerin yasal sorumluluktan kaçmasını, tepki maliyetlerini düşürmesini ve politik, hukuki, teknolojik sınırları sorunsuzca aşmasını sağlamaktadır.7

6.3. Donanım ve Nesnelerin İnterneti (IoT) Temelli Tehditler: 2030'a Doğru

DHI'nın analitik ufku 2030 yılındaki 6G donanım ve iletişim teknolojileri devrimine de işaret etmektedir. Sadece yazılım değil, siber donanımın tasarımı da geleceğin bilişsel harp alanı olacaktır. Örneğin 6G teknolojisinin uluslararası standartlarının Çin liderliğinde belirlenmesi durumunda, kitlesel veri sızdırma (data exfiltration) riskinin doğrudan altyapıya entegre olabileceği endişesi taşınmaktadır.43 Hayatın her alanına giren "Nesnelerin İnterneti" (araçlar, tıbbi cihazlar, akıllı şehir sensörleri vb.), tasarımları itibariyle "mahremiyet merkezli" (privacy baked into design) olmazsa, Uluslararası Telekomünikasyon Birliği'ne (ITU) sunulan "Dijital Nesne Mimarisi" (Digital Object Architecture) tasarısı gibi otoriter gözetim amaçlı eşsiz kayıtlı takip numaralarına dönüşebilir.43 Bu durumda ABD ve müttefik toplumları, fiziksel olarak bir kalıcı total gözetim (total surveillance) ağı içinde yaşayacak ve düşman algı operasyonlarına karşı sonsuz bir kırılganlık taşıyacaklardır.43

7. Stratejik Sonuçlar ve Kurumsal Adaptasyon Gündemi "Bilişsel Üstünlük isteğe bağlı

değildir".5 İncelenen askeri stratejiler, sistem analizleri ve kurum-içi vaka raporları, savaş alanının siber ağlardan çıkıp doğrudan beynin karar merkezlerine taşındığını kanıtlamaktadır.

Defansif Hibrit İstihbarat (DHI) mimarisi bir teorik egzersiz olmaktan öte, medeniyetlerin kendilerini içten çökmeye karşı savunma refleksidir.

Organizasyonel Reform ve Katı Sınırların Yıkılması: Geleneksel bürokrasilerdeki ve özel şirketlerdeki yalıtılmış (silo) departman yapısı acilen terk edilmelidir. Hibrit düşmanlar saldırılarını siber güvenlik zafiyeti, yasal mevzuat boşluğu (lawfare), tedarik zinciri opaklığı (supply chain opacity) ve insan psikolojisini birleştirerek senkronize bir şekilde yürütmektedir.

Buna karşılık, savunma vizyonu "Sistem Yaklaşımı"na (Systems Approach) evrilmelidir. Bu yaklaşım, sadece askeri bir tepki olmaktan çıkıp, tehditleri anlama (understand), esnek şekilde eylem alma (act) ve kurumun yapısını sürekli koşullara uydurma (adapt) döngüsünü zorunlu kılar.48 NATO'nun hibrit faaliyetleri "silahlı saldırı" (armed attack) kapsamına alıp 5. Madde'nin sınırlarına yaklaştırması ve Helsinki Hybrid CoE gibi ortak savunma yapıları inşa etmesi, bu "toplumsal savunma" şuurunun en büyük kanıtıdır.27 Aynı bölgesel esneklik ağlarının Hint-Pasifik bölgesi gibi yüksek siber-gerilimli alanlara teşmil edilmesi tarihi bir gerekliliktir.28 Otomasyon Önyargısı ve Karar Mekanizmalarının Korunması: Tüm stratejik ve askeri kurumlardaki liderler, Yapay Zekâ Karar Destek Sistemlerinin (AI DSS) sağladığı içgörülerin doğasını çok iyi anlamalıdır. Yapay zekâ veri desenlerini okur, bağlamı (context) anlayamaz. CIA örneğinde gördüğümüz üzere 32, karar vermenin ahlaki ve yasal yükü asla bir otonom sisteme devredilemez. Stratejik seviyede liderlerin "Otomasyon Önyargısına" (automation bias) düşmesini engellemek için kurumsal eğitimler (upskilling) ve İstihbarat ajanslarında uygulanan rakip analiz (Team B challenge functions) süreçleri kalıcı hale getirilmelidir.50 Anlamlı İnsan Kontrolü (Meaningful Human Control), yeni alınacak tüm yazılım tedarik süreçlerinin standart ahlaki ve hukuki şablonu olmalıdır.3 Özel Sektör-Devlet Entegrasyonu (DHI Ekosistemi):

Savunma artık sadece üniformalı personelin işi değildir. Devletlerin altyapısı, şirketlerin sunucuları üzerinde durmaktadır. DHI modeli, sivil toplum örgütlerini, çok uluslu şirketleri, lojistik tedarikçileri ve yerel bilgi ekosistemini kapsayan bütünleşik bir bilgi füzyonu gerektirir.

Sivil altyapıyı hedefleyen "epistemik paternalizmin" önüne geçmek, ancak kamuoyunu bilinçlendirerek, orantılı hukuki düzenlemeler çıkararak 20 ve halkı dezenformasyona karşı pasif kurbanlar olmaktan çıkarıp 26 aktif, dirençli ve analitik vatandaşlara dönüştürmekle mümkündür.

bilişsel harp ortamında zafer, bir hedefin fiziksel olarak yok edilmesiyle değil; düşman manipülasyonunun ortasında liderlerin rasyonel, etik ve meşru karar verme (decision-making) becerisinin ve toplumun kurumsal sisteme olan inancının (trust) ayakta kalmasıyla ölçülür.

Hibrit esneklik, teknolojik otomasyon ile insani değerlerin sarsılmaz birlikteliğinde yatmaktadır. Alıntılanan çalışmalar

1. Cognitive Warfare: Definition, Framework, and Case Study - arXiv, erişim tarihi Haziran 3,

2026, https://arxiv.org/html/2603.05222v1

2. Cognitive Warfare: An Allied Blueprint and a Pentagon Opportunity - Small Wars Journal,

erişim tarihi Haziran 3, 2026, https://smallwarsjournal.com/2026/01/16/cognitive-warfare/

3. A Holistic bowtie model of Cognitive Warfare: An interplay of technology, humans,

societies and environment - NATO, erişim tarihi Haziran 3, 2026, https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/ST O-MP-HFM-361/MP-HFM-361-P04.pdf

4. Cognitive Warfare - NATO Science and Technology Organization, erişim tarihi Haziran 3,

2026, https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare -final.pdf

5. Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel..., erişim tarihi Haziran
3, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/437119 5/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/

6. Defensive Hybrid Intelligence | Hybrid Threats, Private Sector, erişim tarihi Haziran 3,
2026, https://www.defensive-hybrid-intelligence.com/

7. New Analysis: Proxies in Hybrid Operations: Insights from the PfPC Workshop in Helsinki,
erişim tarihi Haziran 3, 2026, https://www.pfp-consortium.org/news/new-analysis-proxies-hybrid-operations-insig hts-pfpc-workshop-helsinki

8. Human Agency Under Predictive Insight: Neuroethical Guidance of Behavioral AI -
Medium, erişim tarihi Haziran 3, 2026, https://medium.com/@drjgiordano/human-agency-under-predictive-insight-neuroet hical-guidance-of-behavioral-ai-a772eb8a5456

9. Definitional ambiguity in cognitive warfare: a critical and systematic conceptual review
through ideal-type analysis - Frontiers, erişim tarihi Haziran 3, 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2026.1762571/f ull 10.Definitional ambiguity in cognitive warfare: a critical and systematic conceptual review through ideal-type analysis - Frontiers, erişim tarihi Haziran 3, 2026, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2026.1762571/ pdf

11. Cognitive Competition, Conflict, and War: An Ontological Approach - Amazon S3, erişim
tarihi Haziran 3, 2026, https://s3.amazonaws.com/media.hudson.org/Cognitive+Competition+Conflict+an d+War+-+An+Ontological+Approach+-+Bebber.pdf 12.Cookies settings - ETIS, erişim tarihi Haziran 3, 2026, https://www.etis.ee/Portal/Publications/Display/e661a366-9bbd-4eb6-abad-484da 1e9cb27 13.Holistic Bowtie Model of AI-Based Technology in Defense Systems - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/396050430_Holistic_Bowtie_Model_of_A I-Based_Technology_in_Defense_Systems 14.Mitigating and Responding to Cognitive Warfare - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1200226.pdf 15.Towards a dynamic balance of humans and AI-based systems within our global society and environment -Holistic Bowtie Model of Meaningful Human Control over Effective Systems - ResearchGate, erişim tarihi Haziran 3, 2026, https://www.researchgate.net/publication/380774016_Towards_a_dynamic_balanc e_of_humans_and_AI-based_systems_within_our_global_society_and_environm ent_-Holistic_Bowtie_Model_of_Meaningful_Human_Control_over_Effective_Syst ems 16.Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the Unite - RAND Corporation, erişim tarihi Haziran 3, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA800/RRA853-1/RAND_RRA853-1.pdf 17.Assessing "Cognitive Warfare" | Small Wars Journal by Arizona State University, erişim tarihi Haziran 3, 2026, https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/

18.Lessons-learned with Chinese Characteristics: Understanding the Limits of PLA Efforts to Adapt to Contemporary Warfare - Institute for the Study of War, erişim tarihi

Haziran 3, 2026, https://understandingwar.org/research/china-taiwan/lessons-learned-with-chinese- characteristics-understanding-the-limits-of-pla-efforts-to-adapt-to-contemporary-w arfare/ 19.Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the Unite, erişim tarihi Haziran 3, 2026, https://www.fie.undef.edu.ar/ceptm/wp-content/uploads/2023/06/RAND_RRA853- 1.pdf 20.Principles | Private Sector - Defensive Hybrid Intelligence, erişim tarihi Haziran 3, 2026, https://www.defensive-hybrid-intelligence.com/Principles.html 21.Advancing Human-Machine Teaming: Concepts, Challenges, and Applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2503.16518v1 22.Advancing Human-Machine Teaming: Concepts, Challenges, and Applications - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/pdf/2503.16518 23.Hybrid Intelligence Endpoint Defense (HIED): A Data-Fusion Approach for Proactive Malware Detection - IEEE Xplore, erişim tarihi Haziran 3, 2026, https://ieeexplore.ieee.org/document/11395833/ 24.Modeling the Centaur: Human-Machine Synergy in Sequential Decision Making - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2412.18593v2 25.Designs for Enabling Collaboration in Human-Machine Teaming via Interactive and Explainable Systems - arXiv, erişim tarihi Haziran 3, 2026, https://arxiv.org/html/2406.05003v1 26.Cognitive warfare plays crucial role in countering hybrid threats - NATO admiral - Ukrinform, erişim tarihi Haziran 3, 2026, https://www.ukrinform.net/rubric-ato/4104104-cognitive-warfare-plays-crucial-role-i n-countering-hybrid-threats-says-nato-admiral.html 27.Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/

28.The Case for an EU-NATO Hybrid Centre of Excellence in the Indo-Pacific, erişim tarihi

Haziran 3, 2026,

https://www.iai.it/en/publications/c05/case-eu-nato-hybrid-centre-excellence-indo-p acific 29."Just Being Born": Assessing and Countering Foreign Information Manipulation and Interference (FIMI) in Japan < Sasakawa USA, erişim tarihi Haziran 3, 2026, https://spfusa.org/publications/just-being-born-assessing-and-countering-foreign-in formation-manipulation-and-interference-fimi-in-japan/ 30.Hybrid threats from non-state actors: A taxonomy, erişim tarihi Haziran 3, 2026, https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Rese arch-Report-6-Non-state-actors-WEB.pdf 31.The CIA Is Exploring Human-Machine Security Teaming | FedTech Magazine, erişim tarihi

Haziran 3, 2026,

https://fedtechmagazine.com/article/2025/06/cia-exploring-human-machine-securit y-teaming 32.How the CIA is using generative AI — now and into the future | FedScoop, erişim tarihi Haziran 3, 2026, https://fedscoop.com/how-the-cia-is-using-generative-ai-lakshmi-raman/ 33.CIA Leveraging Digital Transformation Tools in HUMINT Missions - Executive Gov, erişim tarihi Haziran 3, 2026, https://www.executivegov.com/articles/cia-digital-transformation-tools-humint-julian e-gallina 34.AI-enabled Intelligence Digital Ecosystem | PeopleTec, erişim tarihi Haziran 3, 2026, https://www.peopletec.com/blog/ai-enabled-intelligence-digital-ecosystem/ 35.CIA Adds Fourth Pillar to AI Strategy, CAIO Says | GovCIO Media & Research, erişim tarihi Haziran 3, 2026, https://govciomedia.com/cia-adds-fourth-pillar-to-ai-strategy-caio-says/ 36.Deepfake Defense Tech Ready for Commercialization, Transition - DARPA, erişim tarihi Haziran 3, 2026, https://www.darpa.mil/news/2024/deepfake-defense 37.Open Source Tools for Fighting Disinformation - Kitware Inc., erişim tarihi Haziran 3, 2026, https://www.kitware.com/open-source-tools-for-fighting-disinformation/ 38.DARPA Launches New Programs to Detect Falsified Media, erişim tarihi Haziran 3, 2026, https://govciomedia.com/darpa-launches-new-programs-to-detect-falsified-media/

39.MIPs: Modeling Influence Pathways - DARPA, erişim tarihi Haziran 3, 2026, https://www.darpa.mil/research/programs/modeling-influence-pathways 40.AI Forge report - DARPA, erişim tarihi Haziran 3, 2026, https://www.darpa.mil/sites/default/files/attachment/2026-06/ai-forge-report.pdf 41.Cognitive Defense of the Joint Force in a Digitizing World | NSI, erişim tarihi Haziran 3, 2026, https://nsiteam.com/social/cognitive-defense-of-the-joint-force-in-a-digitizing-world 42.Cognitive defense of the Joint Force in a digitizing world - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/pdfs/AD1141773.pdf 43.Intelligent Biology: The Future Character of Information in Strategy: Forged by Cognition and Technology - DTIC, erişim tarihi Haziran 3, 2026, https://apps.dtic.mil/sti/trecms/pdf/AD1154246.pdf 44.The fundamental rights risks of countering cognitive warfare with artificial intelligence - PMC, erişim tarihi Haziran 3, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12500826/ 45.Designing AI-Enabled Countermeasures to Cognitive Warfare - NATO, erişim tarihi

Haziran 3, 2026,

https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/ST O-MP-HFM-377/MP-HFM-377-06.pdf 46.How NATO can integrate AI to prevail in future algorithmic warfare - Atlantic Council, erişim tarihi Haziran 3, 2026, https://www.atlanticcouncil.org/in-depth-research-reports/report/how-nato-can-integrate-ai-to-prevail-in-future-algorithmic-warfare/ 47.The Importance of Cognitive Defense and Cognitive Resilience in, erişim tarihi Haziran 3, 2026, https://spie.org/defense-security/presentation/The-importance-ofcognitive-defense and-cognitive-resiliencein-an-ageof-gen-AIinformation/14049-13 48.Campaigning in the Grey Zone: Towards a Systems Approach to Countering Hybrid Threats, erişim tarihi Haziran 3, 2026, https://www.rand.org/pubs/external_publications/EP70676.html 49.Countering hybrid threats | NATO Topic, erişim tarihi Haziran 3, 2026, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-thr eats

50.Upskilling human actors against AI automation bias in strategic decision making on the resort to force | Cambridge Forum on AI: Law and Governance, erişim tarihi Haziran 3, 2026, https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governa nce/article/upskilling-human-actors-against-ai-automation-bias-in-strategic-decisio n-making-on-the-resort-to-force/75804737BEF096498E05E3EB824A2877 Bölüm Değerlendirme ve Derinleştirme Dosyası

Akademik Derinleştirme Notu

Bu bölümün geniş okuması yapılırken Defansif Hibrit İstihbarat yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası siber, bilişsel, hukuki, algoritmik ve tedarik zinciri füzyonu üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle Defansif Hibrit İstihbarat alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

● ● Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?

- Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi? - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?

- YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı? - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?

- Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı? - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Hibrit İstihbarat ve Nöro-Bilişsel Savunma alanında en güçlü erken uyarı göstergeleri
hangileridir?

2. Bu göstergeler hangi durumda yanlış pozitif üretir?

3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?

4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?

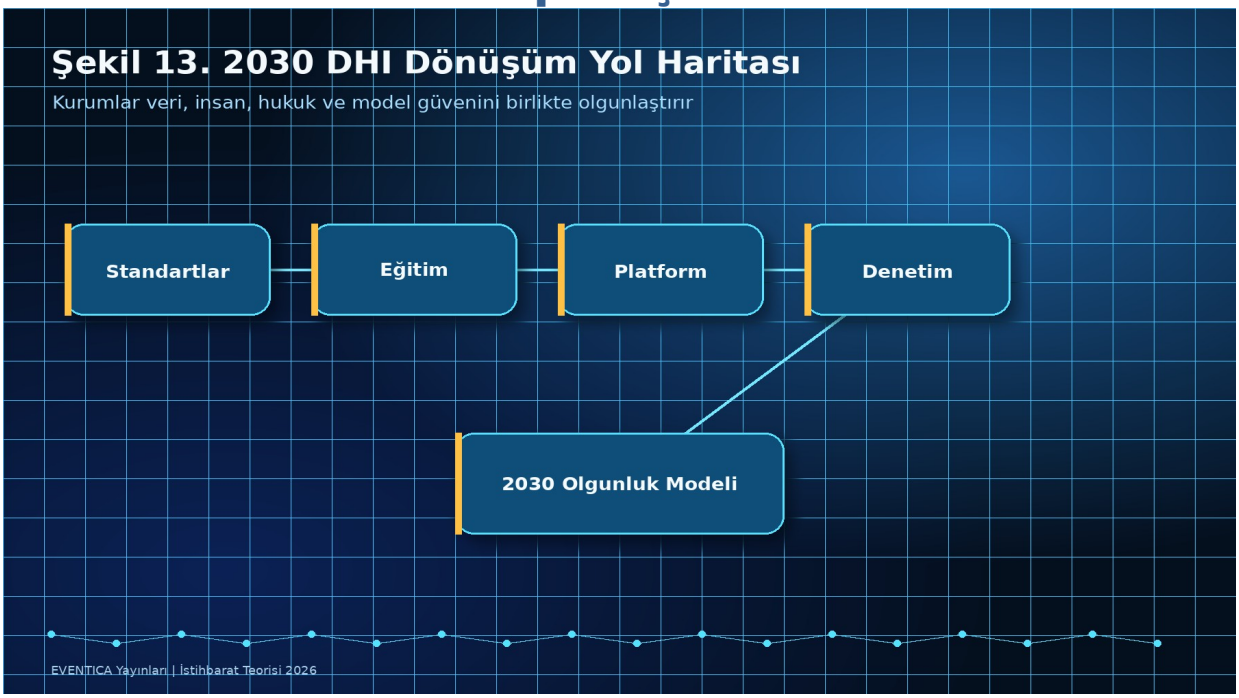
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma
sağlanmalıdır?

6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı
anlamlara gelir?

7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Bölüm 13. Stratejik Sonuçlar, DHI Yol Haritası ve 2030 Kapanışı



Final bölüm, kitabın bütün hatlarını tek bir doktrinel sonuca bağlar: geleceğin istihbaratı hız, doğruluk, güven ve hesap verebilirlik dengesidir.

Şekil 12. Kitabın stratejik kapanışında DHI merkezli kurumsal dönüşüm

Tablo 16. 2030 yol haritası

Dönem	Öncelik	Somut çıktı
2026-2027	Terminoloji ve veri yönetişimi	Ortak sözlük, kaynaklandırma standardı
2027-2028	İnsan-makine karar ortaklığı	DSS denetim protokolleri
2028-2029	Bilişsel dayanıklılık	Erken uyarı ve güven restorasyon programları
2029-2030	DHI olgunluğu	Çapraz alanlı istihbarat merkezi

Final sentez

1. Genel Sonuç

Bu kitabın ana sonucu net: 2026 sonrası istihbarat, tekil rapor üretme işi olmaktan çıkıp sürekli çalışan bir karar mimarisine dönüşmektedir. Bu mimaride veri, insan, yapay zekâ, sosyal

sistemler ve hukuki sorumluluk aynı anda yönetilmek zorundadır. Kurumlar artık sadece daha fazla veri toplayarak üstünlük kuramaz. Asıl üstünlük, veriyi bağlama oturtan, hipotezleri ölçen, bilişsel saldırılara dayanıklı kalan ve karar eşiğini açık tanımlayan yapılarda ortaya çıkar.

2. Doktrinel Kapanış

Klasik istihbarat döngüsü hâlâ değerlidir; fakat artık tek başına yeterli değildir. Gözlem, yönelim, karar ve eylem aşamaları doğrusal bir akış gibi değil, sürekli güncellenen bir ağ gibi çalışmalıdır. OSINT ve ticari veri bu ağın dış sensör katmanını, yapay zekâ modelleme katmanını, Bayesçi muhakeme epistemik kontrol katmanını, DHI ise savunma ve direnç katmanını oluşturur.

3. Kurumsal Tasarım İlkeleri

Bir kurum bu kitabın çizdiği istihbarat mimarisini uygulamak istiyorsa beş ilkeyi merkeze almalıdır. Birincisi, veri kökeni her zaman izlenebilir olmalıdır. İkincisi, yapay zekâ çıktıları karar değil, gerekçelendirilmiş öneri olarak sunulmalıdır. Üçüncüsü, bilişsel güvenlik sadece iletişim biriminin değil, tüm kurumun görevidir. Dördüncüsü, karar destek sistemleri hukuki ve etik filtreyle birlikte tasarlanmalıdır. Beşincisi, her analiz rakip hipotezleri görünür kılmalı ve güven seviyesini açıkça belirtmelidir.

4. 2030 Yol Haritası

2030’a giderken üç eğilim belirleyici olacaktır. İlk eğilim ajan yapay zekâ sistemlerinin kurumsal süreçlere daha derin girmesidir. İkinci eğilim ticari veri ve açık kaynak sensör katmanının stratejik bağımlılık yaratmasıdır. Üçüncü eğilim bilişsel saldırıların daha kişiselleştirilmiş, daha hızlı ve daha zor atfedilebilir hale gelmesidir. Bu üç eğilim birlikte okunduğunda, geleceğin istihbarat kurumu sadece analist yetiştiren değil; veri yönetişimi, model riski, kaynak güvenilirliği, psikolojik dayanıklılık ve hukuki hesap verebilirliği aynı çatı altında yöneten kurum olacaktır.

5. Final Değerlendirme

İstihbarat Teorisi 2026, eski dünyanın gizli bilgi merkezli istihbarat anlayışı ile yeni dünyanın yapay zekâ, bilişsel harp ve hibrit tehdit merkezli güvenlik mimarisi arasında bir geçiş metnidir.

Bu geçişin ana mesajı şudur: İstihbaratın değeri artık sadece bilmekte değil; nasıl bildiğini gösterebilmekte, ne kadar emin olduğunu hesaplayabilmekte ve karar vericiyi hem hız hem de doğruluk bakımından koruyabilmektedir.

öngörmektedir. Geleceğin harp ve istihbarat doktrini, kod satırlarının içinde değil, bu kodların insan yargısı üzerindeki görünmez tahakkümünde yazılmaktadır.

Ek C. Editoryal Üretim ve Kaynak Kullanım Notu

Bu ek, İstihbarat Teorisi 2026 kitabının üretim sürecinde kullanılan editoryal mantığı, kaynak dosya havuzunun nasıl birleştirildiğini ve bölüm

omurgasının hangi ilkelerle düzenlendiğini açıklamak amacıyla hazırlanmıştır.

Bu çalışma, tek bir metnin doğrudan genişletilmesiyle değil; farklı bölüm taslaklarının, akademik raporların, teknik analizlerin, kaynak notlarının ve güncel güvenlik literatürünün ortak bir kitap mimarisi içinde yeniden düzenlenmesiyle oluşturulmuştur. Amaç, dağınık Bölüm dosyalarını ve araştırma notlarını tek bir final kitap omurgasına bağlamak; tekrarları temizlemek, terminolojiyi standartlaştırmak ve bölümler arasında tutarlı bir akademik akış kurmaktır.

Kitabın üretim sürecinde üç temel editoryal ilke izlenmiştir.

Birinci ilke kavramsal standardizasyondur. Aynı kavram farklı dosyalarda farklı adlarla geçtiğinde, kitap boyunca kullanılacak ana terim belirlenmiş ve ilk geçtiği yerde gerekli açıklama yapılmıştır. Bu nedenle **“cognitive warfare”** için bilişsel harp, **“artificial intelligence”** için yapay zekâ / YZ, “open source intelligence” için açık kaynak istihbaratı, “decision support system” için karar destek sistemi ve “defensive hybrid intelligence” için defansif hibrit istihbarat kullanımı tercih edilmiştir.

İkinci ilke içerik bütünleştirmedir. Benzer konular aynı bölüm altında toplanmış, tekrar eden giriş paragrafları azaltılmış, ancak özgün analizler, kavram açıklamaları, tablolar, vaka bağlantıları, sistem mimarileri ve stratejik sonuçlar korunmuştur. Böylece metin, ayrı ayrı yazılmış raporların yan yana dizilmesi yerine tek bir kitap akışı içinde yeniden yapılandırılmıştır.

Üçüncü ilke akademik kitaplaştırmadır. Bölümler yalnızca rapor biçiminde bırakılmamış; giriş, kavramsal çerçeve, analiz, risk değerlendirmesi, tablo/diyagram desteği, sonuç çıkarımı ve bölüm sonu değerlendirme yapısıyla kitap formatına yaklaştırılmıştır. Bu yaklaşım, okuyucunun her bölümü bağımsız bir makale gibi değil, kitabın genel istihbarat teorisi omurgasının bir parçası olarak okumasını sağlar.

Kitap Bölüm Omurgası

Final kitap omurgası 13 bölümden oluşmaktadır. Bu yapı, modern istihbarat teorisini yalnızca klasik bilgi toplama anlayışıyla değil; bilişsel harp, yapay zekâ, OSINT, Bayesçi muhakeme, FIMI, DISARM, karar destek sistemleri, hibrit tehditler ve defansif istihbarat yaklaşımıyla birlikte ele alır.

1. Bölüm 1. İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp
2. Bölüm 2. Sistemik İnvariantlar ve Sosyal Sistemlerin Hedef Alınması
3. Bölüm 3. Yapay Zekâ Destekli Tahmin Sistemleri ve Makine Hızında Karar Alma
4. Bölüm 4. OSINT, Veri Mühendisliği Boru Hatları ve LLM Ajanları
5. Bölüm 5. Davranışsal Modelleme ve Ajan Tabanlı Simülasyonlar
6. Bölüm 6. Siber-Bilişsel Kesişimde FIMI ve DISARM Çerçevesi
7. Bölüm 7. Otonom Hedefleme ve Karar Destek Sistemleri
8. Bölüm 8. Bayesçi İstihbarat: Kanıt, Olasılık ve Hipotez Güncelleme
9. Bölüm 9. Makine Öğrenmesinin İstihbari Epistemolojisi
10. Bölüm 10. Teknolojik Trendler, AGI Projeksiyonları ve Caydırıcılık Boşluğu
11. Bölüm 11. Sosyal Sistemlere Yönelik İstihbarat ve Kurumsal Dayanıklılık
12. Bölüm 12. Hibrit İstihbarat ve Nöro-Bilişsel Savunma
13. Bölüm 13. Stratejik Sonuçlar, DHI Yol Haritası ve 2030 Kapanışı

Bu bölüm yapısı, eski taslaklardaki daha dar üretim planının genişletilmiş ve kitap formatına uyarlanmış final hâlidir. Bayesçi istihbarat bölümü ayrıca eklenmiş; makine öğrenmesi, AGI, sosyal sistemler, hibrit istihbarat ve nöro-bilişsel savunma başlıkları ise daha açık bir bölüm sıralaması içinde yeniden konumlandırılmıştır.

Bilgi Mimarisi

Bu kitabın bilgi mimarisi, konuları birbirinden kopuk başlıklar olarak değil; veri, kavram, analiz ve stratejik sonuç arasında kurulan çok katmanlı bir yapı olarak ele alır.

Birinci katman veri ve gözlem katmanıdır. Bu katmanda açık kaynak verileri, kurumsal raporlar, teknik standartlar, vaka analizleri, akademik literatür ve stratejik güvenlik belgeleri değerlendirilir. Bu katmanın amacı, kitabın teorik

iddialarını yalnızca soyut kavramlara değil, güncel güvenlik ortamındaki somut dönüşümlere de bağlamaktır.

İkinci katman kavramsal entegrasyon katmanıdır. OSINT, FIMI, DISARM, OODA, Bayesçi güncelleme, sistemik invariantlar, karar destek sistemleri, yapay zekâ yönetişimi ve defansif hibrit istihbarat gibi kavramlar bu katmanda birbirine bağlanır. Böylece okuyucu her kavramı yalnızca tanım düzeyinde değil, diğer kavramlarla ilişkisi içinde okuyabilir.

Üçüncü katman analitik ve stratejik sonuç katmanıdır. Bu katmanda, farklı veri ve kavramlardan elde edilen bulgular karar kalitesi, kurumsal dayanıklılık, bilişsel güvenlik, hukuki denetim ve etik sorumluluk açısından değerlendirilir. Kitabın ana iddiası da bu katmanda belirginleşir: 2026 sonrası istihbarat, yalnızca daha fazla veri toplamak değil; verinin güvenilirliğini denetlemek, belirsizlik altında hipotezleri güncellemek ve karar kalitesini koruyabilmektir.

Bu yapı, okuyucunun herhangi bir teknik konuyu yalnızca araç düzeyinde değil; stratejik karar, kurumsal güvenlik, toplumsal dayanıklılık ve etik sorumluluk bağlamında da değerlendirmesini sağlar.

Gerçek Dünya Vakaları, Yapay Zekâ ve İnsan Denetimi

Yapay zekâ destekli karar destek sistemleri, son yıllarda güvenlik ve savunma alanlarında yoğun biçimde tartışılmaktadır. Bu tartışmanın merkezinde yalnızca teknolojik kapasite değil; insan denetimi, veri yanlılığı, hukuki sorumluluk, hata payı, kaynak güvenilirliği ve otomasyon yanlılığı gibi kritik sorunlar yer almaktadır.

Bu kitapta ele alınan vakalar, herhangi bir operasyonel yöntem önermek amacıyla değil; yapay zekâ destekli sistemlerin istihbarat üretimi, karar baskısı, hedef tavsiyesi, veri güvenilirliği ve insan muhakemesi üzerindeki etkilerini etik ve analitik açıdan değerlendirmek için kullanılmaktadır.

Bu nedenle bu bölümün ana sorusu şudur: Yapay zekâ destekli sistemler karar süreçlerini hızlandırırken, insan denetimi, hukuki sorumluluk ve etik sınırlar nasıl korunabilir?

Yapay zekâ destekli karar destek sistemlerinin en önemli riski, insan karar vericinin algoritmik çıktıyı gereğinden fazla güvenilir kabul etmesidir. Otomasyon yanlılığı olarak bilinen bu durum, özellikle zaman baskısı altında çalışan kurumlarda analistin veya karar vericinin kendi muhakemesini geri plana itmesine yol açabilir.

Bu nedenle yapay zekâ destekli karar destek sistemleri yalnızca teknik doğruluk oranlarıyla değil; denetlenebilirlik, açıklanabilirlik, hata yönetimi, kaynak izlenebilirliği ve anlamlı insan kontrolü ilkeleriyle birlikte değerlendirilmelidir. İstihbarat açısından asıl mesele, makinenin hızlı sonuç üretmesi değil; bu sonucun hangi veriyle, hangi varsayımla ve hangi hata payıyla üretildiğinin anlaşılabilmesidir.

FIMI, DISARM ve Bilgi Manipülasyonuna Karşı Savunma Analizi

Dış Bilgi Manipülasyonu ve Müdahalesi, yani FIMI, demokratik süreçleri, toplumsal güveni, kurum meşruiyetini ve karar kalitesini etkileyebilen koordineli bilgi manipülasyonu faaliyetlerini tanımlamak için kullanılan önemli bir kavramdır.

DISARM çerçevesi, bu tür faaliyetleri anlamak ve savunma stratejilerini geliştirmek için kullanılan açık kaynaklı bir analiz modelidir. Bu çalışmada DISARM, saldırı yöntemi öğretmek için değil; manipülasyon örüntülerini tanımak, riskleri sınıflandırmak, savunma reflekslerini güçlendirmek ve kurumsal dayanıklılığı artırmak amacıyla ele alınmaktadır.

FIMI analizinde temel amaç, bir anlatının nasıl yayıldığını yalnızca teknik olarak izlemek değildir. Asıl amaç; hangi toplumsal kırılma hatlarının hedeflendiğini, hangi güven ilişkilerinin aşındırıldığını, hangi platform davranışlarının manipülasyona açık olduğunu ve kurumların bu süreçlere nasıl dayanıklı hâle getirilebileceğini anlamaktır.

Bu bağlamda FIMI ve DISARM, kitapta defansif bir analiz çerçevesi olarak konumlandırılmıştır. Amaç, bilgi ortamındaki riskleri erken fark etmek, sentetik içeriklerin etkisini analiz etmek, kaynak kökenini izlemek, yanlış bilgi yayılımına karşı kurumsal refleksleri geliştirmek ve karar süreçlerinin manipülatif baskılardan korunmasını sağlamaktır.

Trend Analizi: 2020–2026 Döneminin Ana Kırılmaları

2020–2026 dönemi, istihbarat teorisi açısından yalnızca teknik gelişmelerin hızlandığı bir dönem değildir. Aynı zamanda veri, yapay zekâ, açık kaynak istihbaratı, bilişsel güvenlik, platform algoritmaları ve hibrit tehditlerin aynı güvenlik mimarisi içinde birleştiği bir geçiş dönemidir.

Birinci kırılma, açık kaynak istihbaratının kurumsallaşmasıdır. OSINT artık yalnızca internetten bilgi toplama pratiği değildir. Ticari veri, sosyal medya verisi, uydu görüntüleri, teknik kayıtlar, siber tehdit göstergeleri ve kamusal belgeler birlikte değerlendirildiğinde, açık kaynak istihbaratı stratejik karar desteğinin önemli bir parçası hâline gelmiştir.

İkinci kırılma, yapay zekâ destekli analiz sistemlerinin yaygınlaşmasıdır. Yapay zekâ, büyük veri yığınları içinden örüntü çıkarmayı, risk sınıflandırmayı ve tahmin üretmeyi kolaylaştırırken; aynı zamanda denetlenebilirlik, veri yanlılığı, model güvenilirliği ve insan kontrolü sorunlarını da büyütmektedir.

Üçüncü kırılma, bilgi manipülasyonunun ölçek değiştirmesidir. Eski tip bot ağları ve manuel propaganda teknikleri, yerini daha hızlı, daha kişiselleştirilmiş ve daha düşük maliyetli üretken yapay zekâ destekli içerik ekosistemlerine bırakmaktadır. Bu durum, kurumların yalnızca içerik doğrulama değil, anlatı analizi, kaynak kökeni takibi ve bilişsel dayanıklılık kapasitesi geliştirmesini gerekli kılmaktadır.

Dördüncü kırılma, sivil teknolojilerin güvenlik riski üretmesidir. Makine öğrenmesi, enerji, gıda, sağlık, ulaşım ve üretim gibi sivil sektörlerde verimlilik ve otomasyon sağlarken; akıllı altyapılar, endüstriyel kontrol sistemleri, tedarik zincirleri ve karar destek platformları yeni güvenlik bağımlılıkları da üretmektedir. Bu nedenle sivil teknolojiler yalnızca teknik siber güvenlik açısından değil; kurumsal süreklilik, kriz yönetimi, veri yönetişimi ve hibrit tehditler bağlamında da değerlendirilmelidir.

Defansif Hibrit İstihbarat Yaklaşımı

Siber ve bilişsel tehditlerin sürekli, düşük yoğunluklu ve çoğu zaman gri alanlarda yürütülmesi, klasik caydırıcılık anlayışını zorlamaktadır. Bu

nedenle modern güvenlik kurumları yalnızca olay gerçekleştikten sonra tepki veren yapılar olmaktan çıkmalı; erken uyarı, kaynak doğrulama, bilgi ortamı izleme, hukuki denetim ve toplumsal dayanıklılık kapasitesini birlikte geliştirmelidir.

Bu çalışmada önerilen yaklaşım, taarruzi bilgi operasyonları değil; Defansif Hibrit İstihbarat mantığıdır. DHI, siber tehditleri, dezenformasyonu, algoritmik manipülasyonu, sentetik içerikleri, tedarik zinciri risklerini ve hukuki baskı araçlarını tek bir savunma mimarisi içinde ele alır.

Bu mimarinin amacı, hasım aktörlere benzer yöntemlerle karşılık vermek değil; kurumların ve toplumların doğru bilgiye ulaşma, manipülasyonu tanıma, karar kalitesini koruma ve kriz anında güvenilir tepki üretme kapasitesini artırmaktır.

Defansif Hibrit İstihbarat yaklaşımı, yalnızca teknik güvenlik ekiplerinin değil; hukukçuların, analistlerin, iletişim uzmanlarının, veri bilimcilerin, yöneticilerin ve karar vericilerin birlikte çalıştığı bir kurumsal refleks gerektirir. Çünkü modern tehditler tek bir departmana sığmayacak kadar çok katmanlıdır.

Kurumsal Adaptasyon ve Nöro-Bilişsel Dayanıklılık

Bilişsel etki operasyonlarının ulusal güvenlik, kurumsal güven ve toplumsal istikrar üzerindeki sonuçları dikkate alındığında, biliş artık yalnızca bireysel psikoloji meselesi olarak görülemez. Dikkat, güven, algı, muhakeme ve karar süreçleri, modern güvenlik mimarisinin merkezinde yer alan kritik alanlardır.

Bu nedenle kurumlar, bilişsel saldırılara karşı dayanıklılığı test eden ve güçlendiren programlar geliştirmelidir. Bu programlar; medya okuryazarlığı, kaynak doğrulama, kriz iletişimi, yapay zekâ farkındalığı, veri güvenliği, platform davranışı analizi ve karar kalitesi ölçümü gibi alanları birlikte ele almalıdır.

Bu dönüşüm, kurumların hiyerarşik yapısını tamamen ortadan kaldırmak anlamına gelmez. Asıl ihtiyaç, karar süreçlerini yavaşlatan bürokratik kopuklukları azaltmak, disiplinler arası ekipleri güçlendirmek, analistlerin

veri okuryazarlığını artırmak ve teknik ekiplerle karar vericiler arasında daha hızlı geri bildirim kanalları kurmaktır.

Bilişsel dayanıklılık, yalnızca yanlış bilgiyi düzeltme refleksi değildir. Daha geniş anlamda, kurumların ve toplumların belirsizlik altında doğru soruları sorabilmesi, kanıtı tartabilmesi, hipotezlerini güncelleyebilmesi ve manipülatif baskılara rağmen karar kalitesini koruyabilmesidir.

Sonuç

İstihbarat Teorisi 2026, en çok veriye sahip olan aktörün değil; verinin güvenilirliğini denetleyebilen, belirsizlik altında hipotezlerini güncelleyebilen, yapay zekâ destekli sistemlerin sınırlarını anlayabilen ve kendi kurumlarının bilişsel dayanıklılığını koruyabilen aktörlerin daha güçlü olacağını savunur.

Geleceğin istihbarat anlayışı yalnızca kodda, sensörde veya algoritmada şekillenmeyecektir. Asıl belirleyici olan, bu teknolojilerin insan muhakemesi, hukuk, etik, kurumsal denetim ve toplumsal güven üzerindeki etkilerini doğru yönetebilme kapasitesidir.

Bu nedenle kitap, modern istihbaratı yalnızca bilgi toplama faaliyeti olarak değil; veri, insan muhakemesi, yapay zekâ, bilişsel güvenlik, hukuki denetim ve kurumsal dayanıklılık arasında kurulan çok katmanlı bir karar mimarisi olarak ele alır.

Kaynakça ve Seçilmiş Okuma Listesi

Bu bölümde yer alan kaynaklar; istihbarat çalışmaları, açık kaynak istihbaratı, yapay zekâ yönetişimi, siber güvenlik, bilişsel harp, hibrit tehditler, hukuk, etik ve stratejik analiz alanlarında kullanılan temel belge, rapor, akademik çalışma ve teknik çerçevelerden oluşmaktadır.

Kaynaklar yalnızca metni desteklemek için değil, okuyucunun konuyu daha derinlemesine takip edebilmesi için de seçilmiştir. Resmî doktrin belgeleri, uluslararası standartlar, akademik yayınlar ve güncel politika raporları ayrı başlıklar altında değerlendirilmiştir.

1. Cognitive Warfare - NATO, erişim tarihi Haziran 2, 2026,

https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/S TO-MP-HFM-361/MP-HFM-361-P17P.pdf

2. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory

concept - PMC, erişim tarihi Haziran 2, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/

3. An Artificial Intelligence/Machine Learning Perspective on Social Simulation: New Data

and New Challenges - RAND, erişim tarihi Haziran 2, 2026, https://www.rand.org/content/dam/rand/pubs/working_papers/WR1200/WR1213/RAND_WR1213.pdf

4. An OSINT-driven architecture for digital asset discovery and risk evaluation -

CEUR-WS.org, erişim tarihi Haziran 2, 2026, https://ceur-ws.org/Vol- 4180/Paper1.pdf

5. Technical Architecture Analysis of IntellyWeave OSINT Platform | by..., erişim tarihi
Haziran 2, 2026, https://medium.com/@geolibra/technical-architecture- analysis-of-intellyweave-osint-platform-6bdd4bf3d220

6. 4th EEAS Report on Foreign Information Manipulation and Interference Threats -
European Union, erişim tarihi Haziran 2, 2026, https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf

7. DISARM Framework - "Mendeleev's table" of information operations and campaigns,
erişim tarihi Haziran 2, 2026, https://project-athena.eu/disarm- framework-mendeleevs-table-of-information-operations-and-campaigns/

8. AI-assisted targeting in the Gaza Strip - Wikipedia, erişim tarihi Haziran 2, 2026,
https://en.wikipedia.org/wiki/AI-assisted_targeting_in_the_Gaza_Strip

9. The proliferation of AI-enabled military technology in the Middle East, erişim tarihi
Haziran 2, 2026, https://www.iiss.org/online-analysis/charting-middle-east/2026/04/the-proliferation-of-ai-enabled-military-technology-in-the- middle-east/

10. [2501.04894] A Look into How Machine Learning is Reshaping Engineering Models: the
Rise of Analysis Paralysis, Optimal yet Infeasible Solutions, and the Inevitable Rashomon Paradox - arXiv, erişim tarihi Haziran 2, 2026, https://arxiv.org/abs/2501.04894

11. Artificial General Intelligence Forecasting and Scenario Analysis - RAND, erişim tarihi
Haziran 2, 2026, https://www.rand.org/pubs/research_reports/RRA4692- 1.html

12. offset-x | scsp, erişim tarihi Haziran 2, 2026, https://www.scsp.ai/wp-
content/uploads/2023/05/Offset-X-Closing-the-Detterence-Gap-and-Building- the-Future-Joint-Force.pdf

13. The significance of AI and ML in OSINT to human investigators - ShadowDragon®, erişim
tarihi Haziran 2, 2026, https://shadowdragon.io/resources/ai-ml-and- human-intelligence-in-the-intelligence-analysis-process/

14. The Cognitive Warfare Concept Cognitive warfare is now seen as its own domain in
modern warfare. Alongside the four military dom, erişim tarihi Haziran 2, 2026, https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie- du-Cluzel-final_0.pdf

15. Cognitive Warfare - NATO's ACT, erişim tarihi Haziran 2, 2026,
https://www.act.nato.int/activities/cognitive-warfare/

16. Cognitive warfare: NATO chief scientist research report, erişim tarihi Haziran 2, 2026,
https://www.sto.nato.int/wp-content/uploads/chief-scientist-report- cognitive-warfare-final.pdf

17. New CCDCOE research reconceptualises cognitive warfare, erişim tarihi Haziran 2, 2026,
https://ccdcoe.org/news/2026/new-ccdcoe-research-reconceptualises- cognitive-warfare/

18. Influence Operations in Social Networks - arXiv, erişim tarihi Haziran 2,
2026, https://arxiv.org/html/2502.11827v1

19. Dismantling the Foreign Information Manipulation and Interference (FIMI) house of
cards, erişim tarihi Haziran 2, 2026, https://www.eeas.europa.eu/eeas/dismantling-infrastructure-foreign- information-manipulation-and-interference-house-cards_en

20. Foreign Information Manipulation and Interference - Institute for Strategic Dialogue,
erişim tarihi Haziran 2, 2026, https://www.isdglobal.org/our- expertise/information-warfare-and-online-manipulation/foreign-information- manipulation-and-interference/

21. Nicolas99-9/llm-agent-simulation-papers - GitHub, erişim tarihi Haziran 2, 2026,
https://github.com/Nicolas99-9/llm-agent-simulation-papers

22. The Power of Data-Driven Behavior Engineering: Crack the Success Code - Medium,
erişim tarihi Haziran 2, 2026, https://medium.com/@nomannayeem/the- power-of-data-driven-behavior-engineering-crack-the-success-code- 7ce8b6328f3e

23. Social Media Information Operations - PubsOnLine, erişim tarihi Haziran 2, 2026,
https://pubsonline.informs.org/doi/10.1287/educ.2025.0289

24. 1 Introduction - arXiv, erişim tarihi Haziran 2, 2026,
https://arxiv.org/html/2508.01552v1

25. Training Data Influence Analysis and Estimation: A Survey - arXiv, erişim tarihi Haziran 2,
2026, https://arxiv.org/pdf/2212.04612

26. D4.2 OSINT data fusion and analysis architecture - European Union, erişim tarihi
Haziran 2, 2026,

https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b8f84b9f&appId=PPGMS

27. Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment,
erişim tarihi Haziran 2, 2026, https://www.mdpi.com/2073- 431X/14/10/430

28. [2602.21193] On Data Engineering for Scaling LLM Terminal Capabilities - arXiv, erişim
tarihi Haziran 2, 2026, https://arxiv.org/abs/2602.21193

29. What is Predictive Modeling? Types & Techniques - Qlik, erişim tarihi Haziran 2, 2026,
https://www.qlik.com/us/predictive-analytics/predictive-modeling

30. What Is Predictive Modeling? Models, Benefits, and Algorithms | NetSuite, erişim tarihi
Haziran 2, 2026, https://www.netsuite.com/portal/resource/articles/financial-management/predictive-modeling.shtml

31. The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis,
erişim tarihi Haziran 2, 2026, https://www.csis.org/analysis/analytic- edge-leveraging-emerging-technologies-transform-intelligence-analysis

32. What is Predictive Modeling? An Introduction - Splunk, erişim tarihi Haziran 2, 2026,
https://www.splunk.com/en_us/blog/learn/predictive-modeling.html

33. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy,
Information, and Resilience - CSIS, erişim tarihi Haziran 2, 2026, https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age- autonomy-information-and-resilience

34. Data Science Engineers and Their Role in Predictive Analytics - Focus GTS, erişim tarihi
Haziran 2, 2026, https://www.focusgts.com/predictive-analytics-how-data- science-engineers-drive-it-forecasting/

35. 'The Gospel': how Israel uses AI to select bombing targets in Gaza - The Guardian,
erişim tarihi Haziran 2, 2026, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses- ai-to-select-bombing-targets

36. The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose - RUSI, erişim
tarihi Haziran 2, 2026, https://www.rusi.org/explore-our-research/publications/commentary/israel-defense-forces-use-ai-gaza-case- misplaced-purpose

37. 4th EEAS Report on FIMI Threats – Dismantling the FIMI house of cards - EUvsDisinfo,
erişim tarihi Haziran 2, 2026, https://euvsdisinfo.eu/4th-eeas-report- on-fimi-threats-dismantling-the-fimi-house-of-cards/

38. An Agentic Operationalization of DISARM for FIMI Investigation on Social Media - arXiv,
erişim tarihi Haziran 2, 2026, https://arxiv.org/html/2601.15109v2

39. Framework - DISARM Foundation, erişim tarihi Haziran 2, 2026,
https://www.disarm.foundation/framework

40. Introducing DISARM - Disinformation Analysis and… - Alfred Landecker Stiftung, erişim
tarihi Haziran 2, 2026, https://www.alfredlandecker.org/en/article/introducing-disarm-disinformation- analysis-and-risk-management

41. An introduction to DISARM Framework on disinformation tactics, techniques and
procedures – First session - EDMO, erişim tarihi Haziran 2, 2026, https://edmo.eu/training/an-introduction-to-disarm-framework-on- disinformation-tactics-techniques-and-procedures-first-session/

42. [2502.11827] Influence Operations in Social Networks - arXiv, erişim tarihi
Haziran 2, 2026, https://arxiv.org/abs/2502.11827

43. (PDF) Influence Operations in Social Networks - ResearchGate, erişim tarihi Haziran 2,
2026, https://www.researchgate.net/publication/389091197_Influence_Operations_in_Social_Networks

44. Quantifying the vulnerabilities of the online public square to adversarial manipulation
tactics, erişim tarihi Haziran 2, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC11238850/

45. 7. Social Media and Influence Operations Technologies: Implications for Great Power
Competition - NDU Press, erişim tarihi Haziran 2, 2026, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404329/7- social-media-and-influence-operations-technologies-implications-for-great- pow/

46. PEACEKEEPING IN AN ERA OF CONVERGING TECHNOLOGICAL & SECURITY THREATS -
United Nations Peace Operations, erişim tarihi Haziran 2, 2026, https://mineaction.org/sites/default/files/06_24_final_pauwels_converging_ai_cyberthreats_digital_peacekeeping_strategy_1.pdf

47. THE WEAPONIZATION OF ARTIFICIAL INTELLIGENCE THE NEXT STAGE OF TERRORISM
AND WARFARE - COE-DAT, erişim tarihi Haziran 2, 2026, https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf

48. ARTIFICIAL INTELLIGENCE: At the Unit of Action, erişim tarihi Haziran 2, 2026,
https://d34w7g4gy10iej.cloudfront.net/pubs/pdf_76851.pdf

49. Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel..., erişim tarihi
Haziran 2, 2026, https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4371195/cognitive-warfare-2026-natos-chief-scientist- report-as-sentinel-call-for-operat/

50. “Addressing the National Security Implications of Artificial Intelligence: People,

Bureaucracy, and Data Infrastructure”, erişim tarihi Haziran 2, 2026, https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default- files-documents-os-bjensen-091923.pdf

51. Defensive Hybrid Intelligence | Hybrid Threats, Private Sector, erişim tarihi Haziran 2,

2026, https://www.defensive-hybrid-intelligence.com/ Bölüm Değerlendirme ve Derinleştirme Dosyası

Akademik Derinleştirme Notu

Bu bölümün geniş okuması yapılırken stratejik yol haritası yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası kurumsal adaptasyon, 2030 hazırlığı, veri yönetişimi ve hesap verebilirlik üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir.

Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar.

Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle stratejik yol haritası alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Değerlendirme ve Derinleştirme Dosyası

Derinlemesine Analiz

Bu bölümün geniş okuması yapılırken stratejik yol haritası yalnızca teorik bir kavram olarak ele alınmamalıdır. İstihbarat açısından kritik nokta, kavramın hangi veriyle beslendiği, hangi hipotezi güçlendirdiği, hangi karar eşiğine bağlandığı ve hangi kurumsal riskleri görünür hale getirdiğidir. Bu nedenle bölümün analitik omurgası kurumsal adaptasyon, 2030 hazırlığı, veri yönetişimi ve hesap verebilirlik üzerinden kurulmalıdır. Böyle bakıldığında metin, sadece alan yazını özeti olmaktan çıkar; karar vericiye doğrudan bağlanabilen bir analiz mimarisine dönüşür.

Uygulama düzeyinde ilk adım, kavramı ölçülebilir göstergelere ayırmaktır. Her gösterge için kaynak türü, veri güvenilirliği, güncellik, manipülasyon riski ve rakip hipotezlerle ilişkisi ayrı ayrı yazılmalıdır. İkinci adım, göstergelerin tek tek değil birlikte nasıl davrandığını görmektir. Modern istihbaratta en tehlikeli hata, tek bir güçlü sinyali mutlak kanıt gibi okumaktır. Oysa çoğu zaman asıl değer, zayıf sinyallerin aynı yöne mi işaret ettiği, yoksa birbirini boşa mı düşürdüğü sorusundadır.

Bu bölümden üretilecek bir istihbarat ürünü en az altı alan içermelidir: ana hipotez, rakip hipotezler, kullanılan kaynak ailesi, kanıt ağırlığı, güven seviyesi ve önerilen karar eşiği. Bu format, kurum içinde hem analitik kaliteyi artırır hem de sonradan denetlenebilirlik sağlar. Karar verici açısından önemli olan sadece “ne düşünüyoruz?” cevabı değildir. En az onun kadar önemli olan “bunu neden düşünüyoruz, ne kadar eminiz ve hangi durumda fikrimizi değiştiririz?” sorusudur.

Risk yönetimi tarafında üç kırılganlık öne çıkar. Birincisi veri körlüğüdür; yani kurumun sadece kolay eriştiği veriye güvenmesi. İkincisi model körlüğüdür; yani analitik aracın ürettiği sonucu bağlamdan bağımsız kabul etmesi. Üçüncüsü kurum körlüğüdür; yani bürokratik alışkanlıkların yeni tehdit biçimlerini eski kategoriyle okumaya zorlamasıdır. Bu üç risk özellikle stratejik yol haritası alanında birlikte çalışır ve analizi sessiz biçimde zayıflatır.

Bu yüzden her bölüm sonunda kullanılabilecek pratik kontrol şu şekildedir: Verinin kökeni açık mı? Kanıt bağımsız mı? Alternatif açıklama var mı? Model veya yorum hangi varsayıma yaslanıyor? Hukuki ve etik sınır nerede başlıyor? İnsan denetimi gerçek mi, yoksa sadece prosedürel bir

imza mı? Sonuç hangi karar eşiğine bağlanıyor? Bu sorular cevaplanmadan üretilen her istihbarat ürünü eksik kalır.

Son olarak, bu bölümün 2026 sonrası değeri kurumsal öğrenme kapasitesidir. İyi kurumlar her raporu tek seferlik çıktı olarak görmez. Raporu aynı zamanda modelini, varsayımını ve karar eşiğini test eden bir öğrenme nesnesi olarak kullanır. Başarılı tahminler kadar hatalı tahminler de arşivlenir, sınıflandırılır ve sonraki analizde kullanılır. Böylece istihbarat üretimi kişisel sezgiden kurumsal hafızaya, dağınık veriden ölçülebilir muhakemeye doğru ilerler.

Bölüm Sonu Kontrol Listesi

- Ana kavram açık tanımlandı mı ve diğer bölümlerdeki kullanımla uyumlu mu?
  - Veri kaynağı, kaynak kökeni ve güven seviyesi ayrı ayrı belirtildi mi?
  - Rakip hipotezler gerçekten zorlandı mı, yoksa sadece ana iddiayı destekleyen kanıtlar mı seçildi?
  - YZ veya model çıktısı varsa, bunun hangi varsayımla çalıştığı açıklandı mı?
  - Analiz, karar vericinin kullanabileceği somut eşiğe bağlandı mı?
  - Hukuki, etik ve kurumsal riskler metnin sonunda değil, analizin içinde mi ele alındı?
  - Bu bölümden üretilecek istihbarat ürünü daha sonra denetlenebilir mi?

Araştırma Soruları

1. Stratejik Sonuçlar, DHI Yol Haritası ve 2030 Kapanışı alanında en güçlü erken uyarı göstergeleri hangileridir?
2. Bu göstergeler hangi durumda yanlış pozitif üretir?
3. Kanıtların birbirinden bağımsız olduğu nasıl test edilir?
4. İnsan analist ile yapay zekâ sistemi arasında görev paylaşımı nasıl kurulmalıdır?
5. Aynı veriyle çalışan iki farklı analist farklı sonuca varırsa hangi yöntemle uzlaşma sağlanmalıdır?
6. Bu bölümdeki kavramlar Türkiye, NATO ve küresel güvenlik ekosistemi açısından hangi farklı anlamlara gelir?
7. Kurumsal uygulama için minimum veri, personel, hukuk ve teknoloji kapasitesi nedir?

8. 2030’a giderken bu alanın en büyük bilinmeyeni hangi başlıkta toplanmaktadır?

Ekler

Ek A. Kavram Sözlüğü

Tablo 17. Genişletilmiş kavram sözlüğü

Terim	Tanım
Bilişsel Harp	Algı, dikkat, güven, muhakeme, kimlik ve karar süreçlerini hedef alan çatışma biçimi.
FIMI	Dış Bilgi Manipülasyonu ve Müdahalesi; dış aktör kaynaklı koordineli bilgi manipülasyonu.
DHI	Defansif Hibrit İstihbarat; siber, bilişsel, hukuki, algoritmik ve tedarik zinciri risklerini birlikte ele alan savunma yaklaşımı.
OSINT	Açık kaynaklardan üretilen istihbarat; kamusal ve bazı ticari erişilebilir veri katmanlarını kapsar.
DSS	Karar Destek Sistemi; insan karar vericiye seçenek, risk ve öncelik üreten analitik mimari.
OODA	Gözlem, Yönelim, Karar, Eylem döngüsü; modern yapıda doğrusal değil ağ tabanlı çalışır.
Bayesçi Güncelleme	Yeni kanıtla hipotez olasılığının sistematik biçimde güncellenmesi.
Rashomon Etkisi	Aynı veri setini açıklayan birden fazla tutarlı modelin bulunması durumu.
Ajan Yapay Zekâ	Hedefleri alt görevlere bölebilen, araç kullanabilen ve sınırlı otonomiyle ilerleyebilen YZ yapısı.
Sistemik İnvariant	Bir sosyal sistemin şoklara rağmen kimliğini ve koordinasyon kapasitesini koruyan değişmez yapı

Terim	Tanım
	taşı.
Kill Web	Hedefleme ve ateş gücü bağlantılarının doğrusal zincir yerine ağ mantığıyla çalışması.
Sensemaking	Veri ve olayların karar verici için anlamlı bir çerçeveye oturtulması.
Kaynak kökeni / provenance	Bir verinin nereden geldiği, nasıl işlendiği ve hangi dönüşümlerden geçtiği bilgisi.
Anlamlı insan kontrolü	Makine önerisinin gerçek insan denetimi, gerekçe okuma ve sorumluluk süzgecinden geçmesi.
Güven seviyesi	Analistin sonuca ne kadar emin olduğunu gösteren nitel veya nicel değerlendirme.

Kaynak Dosya Havuzu ve İnternet Destekli Kaynaklar

Bu bölüm, kitabın üretiminde kullanılan ana dosya havuzunu ve metni destekleyen güncel açık kaynak/kurumsal internet referanslarını toplu biçimde gösterir. **Liste, yayınevi arşivi ve akademik şeffaflık amacıyla eklenmiştir.**

A. Kullanılan Dosya Havuzu

No	Dosya	Kitaptaki Kullanım
1	İstihbarat Teorisi 2026 Kitap Üretim Planı.pdf	Kitap mimarisi, bölüm akışı ve üretim planı
2	İstihbarat Teorisi 2026.docx	Ana kitap omurgası ve birleştirme gövdesi
3	İstihbaratın Ontolojik Dönüşümü ve Bilişsel Harp.docx	Bölüm 1 ve bilişsel harp dönüşümü
4	Bilişsel Harp_ İstihbaratın Dönüşümü.pdf	Bilişsel harp ve bilgi ortamı analizleri
5	Sosyal Sistemlere Yönelik İstihbarat Analizi.pdf	Bölüm 2 ve Bölüm 11 sosyal sistem dayanıklılığı
6	Yapay Zekâ Tahmin Sistemleri Stratejik Analizi.pdf	Bölüm 3 YZ destekli tahmin sistemleri
7	OSINT, LLM ve Stratejik İstihbarat Analizi.pdf	Bölüm 4 OSINT, LLM ve veri mühendisliği hattı
8	Davranışsal Modelleme ve Yapay Zekâ Simülasyonları.pdf	Bölüm 5 davranışsal modelleme ve ajan simülasyonları

9	Siber-Bilişsel FIMI_ DISARM Çerçevesi Analizi.pdf	Bölüm 6 FIMI ve DISARM analizi
10	Otonom Hedefleme ve DSS Araştırma Raporu.pdf	Bölüm 7 karar destek ve insan denetimi
11	makine öğrenmesi İstihbarat Epistemolojisi Analizi.pdf	Bölüm 9 epistemoloji, Rashomon etkisi ve model güveni
12	AGI, Hibrit Tehditler ve Caydırıcılık Analizi.pdf	Bölüm 10 AGI, trendler ve caydırıcılık boşluğu
13	Hibrit İstihbarat ve Nöro-Bilişsel Savunma Analizi.pdf	Bölüm 12 ve Bölüm 13 DHI / nöro-bilişsel savunma

B. İnternet Destekli Birincil / Kurumsal Kaynaklar

Kaynak	Kitaptaki Katkı	Adres
ODNI IC OSINT Strategy 2024-2026	OSINT'in kurumsal kabiliyet ve açık/ticari veri hattı olarak konumlandırılması	https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf
NIST AI RMF / Generative AI Profile	YZ risk yönetimi, güvenilirlik, ölçme, yönetişim ve kontrol mantığı	https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
European Commission – AI Act	AB AI Act yürürlük ve uygulama takvimi; yüksek riskli YZ sistemleri	https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
NATO STO – Cognitive Warfare	Bilişsel harp, insan zihni, güven ve karar mimarisi tartışmaları	https://www.sto.nato.int/wp-content/uploads/chief-scientist-report-cognitive-warfare-final.pdf
MITRE ATT&CK	Siber tehdit istihbaratı, TTP haritalama ve savunma modelleme	https://attack.mitre.org/
OASIS STIX/TAXII 2.1	Siber tehdit istihbaratı paylaşımı ve birlikte işlerlik standardı	https://www.oasis-open.org/2021/06/23/stix-v2-1-and-taxii-v2-1-oasis-standards-are-published/
NGA GEOINT	Coğrafi istihbarat tanımı ve görüntü/coğrafi veri analizi	https://www.nga.mil/about/About_Us.html
DISARM Framework	Dezenformasyon ve etki operasyonlarını haritalama dili	https://www.disarm.foundation/framework

C. Formül Kontrol Notu

Bayes formülü kitapta Bölüm 8 içinde ayrıca korunmuştur: $P(H|E) = [P(E|H) \times P(H)] / P(E)$.

XGBoost objektif fonksiyonu kitapta makine öğrenmesi ve risk skorlama bağlamında görünür biçimde verilmiştir: $Obj = \Sigma_i\, l(y_i, \hat{y}_i) + \Sigma_k\, \Omega(f_k)$.

Etkileşim Verimliliği ve Rashomon kümesi formülleri de Formüller Listesi ile ilgili bölümlerde ayrıca gösterilmiştir.

Kapanış Notu

Bu final kitap metni, bölüm dosyalarının doğrudan yığılması şeklinde değil; ortak kavram çizgisi, bölüm akışı, tablo/diyagram desteği ve Bayesçi

muhakeme ek bölümüyle birlikte yeniden kurulmuş bütünleşik bir akademik kitap taslağı olarak hazırlanmıştır.